

2004

# Applying Security Risk Management to Internet Connectivity in K-12 Schools and School Districts

Carol C. Woody

*Nova Southeastern University*, [ccwoody@att.net](mailto:ccwoody@att.net)

This document is a product of extensive research conducted at the Nova Southeastern University [College of Engineering and Computing](#). For more information on research and degree programs at the NSU College of Engineering and Computing, please click [here](#).

Follow this and additional works at: [https://nsuworks.nova.edu/gscis\\_etd](https://nsuworks.nova.edu/gscis_etd)



Part of the [Computer Sciences Commons](#)

## Share Feedback About This Item

---

### NSUWorks Citation

Carol C. Woody. 2004. *Applying Security Risk Management to Internet Connectivity in K-12 Schools and School Districts*. Doctoral dissertation. Nova Southeastern University. Retrieved from NSUWorks, Graduate School of Computer and Information Sciences. (933)

[https://nsuworks.nova.edu/gscis\\_etd/933](https://nsuworks.nova.edu/gscis_etd/933).

This Dissertation is brought to you by the College of Engineering and Computing at NSUWorks. It has been accepted for inclusion in CEC Theses and Dissertations by an authorized administrator of NSUWorks. For more information, please contact [nsuworks@nova.edu](mailto:nsuworks@nova.edu).

Applying Security Risk Management to  
Internet Connectivity in K-12 Schools and School Districts

by

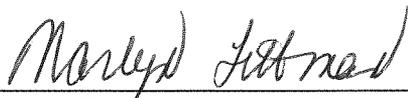
Carol C. Woody

A dissertation submitted in partial fulfillment of the requirements  
for the degree of Doctor of Philosophy

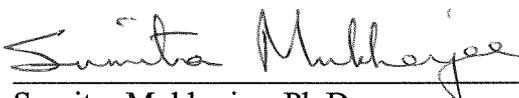
Graduate School of Computer and Information Sciences  
Nova Southeastern University

2004

We hereby certify that this dissertation, submitted by Carol C. Woody, conforms to acceptable standards and is fully adequate in scope and quality to fulfill the dissertation requirements for the degree of Doctor of Philosophy.

  
\_\_\_\_\_  
Marlyn Kemper Littman, Ph.D.  
Chairperson of Dissertation Committee

April 29, 2004  
Date

  
\_\_\_\_\_  
Sumitra Mukherjee, Ph.D.  
Dissertation Committee Member

4/29/2004  
Date

  
\_\_\_\_\_  
Gertrude Abramson, Ed.D.  
Dissertation Committee Member

April 29, 2004  
Date

Approved:

  
\_\_\_\_\_  
Edward Liebein, Ph.D.  
Dean, Graduate School of Computer and Information Sciences

4-29-04  
Date

Graduate School of Computer and Information Sciences  
Nova Southeastern University

An Abstract of a Dissertation Submitted to Nova Southeastern University  
in Partial Fulfillment of the Requirements for the Degree of Doctor of Philosophy

## Applying Security Risk Management to Internet Connectivity in K-12 Schools and School Districts

by  
Carol C. Woody

April 2004

Internet connectivity has been added to the classrooms of United States (U.S.) K-12 schools, but recognition of the security risks and related management responsibilities to address increased risk exposure is not apparent. Providing a sufficient level of access for K-12 students to learn through exploration and experimentation needs to be balanced with sufficient limitations to minimize the risk of technically proficient participants inflicting harm through school resources. Problems of inappropriate use such as adjusting grades, tampering with work of other students, and defacing Web sites by K-12 students are already appearing in U.S. newspapers. In addition, the growing level of Internet security incidents such as worms and malicious code puts K-12 technology infrastructure and data at risk.

Each K-12 school and school district has a unique set of technical capabilities that must be balanced against the risk of misuse to establish appropriate security. Applying security risk management can allow K-12 administrators to identify areas of weak security that pose unacceptable risk and plan for needed improvements. Within this investigation, a security risk methodology was selected, tailored to incorporate organizational characteristics and regulatory requirements unique to K-12 schools and school districts, and successfully applied by the Scarsdale Public School District, Scarsdale, New York. In addition, several K-12 school officials including school board members, technology directors, and superintendents, reviewed the tailored methodology and affirmed its applicability to their schools and school districts.

The Operationally Critical Threat, Asset, and Vulnerability Evaluation<sup>SM</sup> (OCTAVE®) Methodology was selected by this investigator for evaluating the security risk of K-12 schools and school districts. The OCTAVE Methodology applies a security risk management approach developed by researchers at the Carnegie Mellon® Software Engineering Institute (SEI<sup>SM</sup>). The methodology is used by over 1,000 medical, financial, manufacturing, and government organizations, and allows for self-direction. It is available at no cost and provides a wide range of tailoring capabilities for adapting

---

<sup>SM</sup> Operationally Critical Threat, Asset, and Vulnerability Evaluation and SEI are service marks of Carnegie Mellon University.

® OCTAVE and Carnegie Mellon are registered in the U.S. Patent and Trademark Office.

security risk management to unique domains. As a result, the OCTAVE Methodology provided a reasonable option for validating the use of security risk management in K-12 schools and school districts.

## Acknowledgments

The guidance of my chairperson, Dr. Marlyn Littman, has been invaluable in shaping the direction and structure of this research. The time and attention provided by my committee members Dr. Sumitra Mukherjee and Dr. Gertrude Abramson in reviewing my research documents at multiple points throughout the development process is greatly appreciated.

I am extremely grateful for the effort provided by Gerald Crisci, Director of Computer Science Curriculum for the Scarsdale Public School District, and the members of the analysis team who joined him in validating the methodology. Their insights and suggestions added greatly to the usability of the resulting product.

My thanks to Keith Krueger, Executive Director for the Consortium for School Networking (CoSN), who saw the potential of my ideas and put me in touch with others at CoSN to help me along. Steve Miller, Executive Director for Mass Networks and an advocate for K-12 Internet security on the CoSN Executive Board, was a great help in preparing my ideas for broad use.

Many thanks to a tireless cadre of family and friends whose interest and gentle persistence kept this researcher focused on the end goal of completing this dissertation.

Words are insufficient to express my gratitude to my husband, Robert, who juggled the daily complexities of our lives and listened to my grumbles while I struggled with the dissertation process.

# Table of Contents

Abstract iii

## Chapters

- 1. Introduction 1**
  - Statement of the Problem Investigated and Goal That Was Achieved 1
    - Technology Use in Education 1
    - Internet Context 2
    - Risk for Children Using the Internet 4
    - Risks for K-12 Schools and School Districts with Internet Access 8
  - Relevance and Significance 14
    - Internet Content Filtering 16
    - Internet Risks Not Addressed by Content Filtering 23
    - Security Risk Management 29
  - Barriers and Issues 33
  - Limitations and Delimitations of the Study 37
  - Definition of Terms 40
  - Summary 43
- 2. Review of the Literature 46**
  - Historical Overview of the Research Literature 46
    - Use of Technology in Schools 47
      - Measuring Technology Value 47
      - Legislative Mandates 50
    - Protection for Children Using the Internet 53
    - Security Risk Management and the OCTAVE Approach 56
    - OCTAVE and Other Security Risk Methodologies 61
  - Research Literature Specific to the Topic 63
  - Summary of What Is Known and Unknown About the Topic 71
  - The Contribution this Study Makes to the Field 74
- 3. Methodology 77**
  - Research Method Employed 77
    - OCTAVE Methodology Description 81
      - Phase 1: Organizational View 82
      - Phase 2: Technological View 83
      - Phase 3: Security Strategy and Planning 84
    - OCTAVE Criteria Principles 86
      - Principles from Security Risk Management 87
      - Principles from Risk Management 88
      - Principles from Organizational Management 88
    - OCTAVE Criteria Attributes 89
      - Attributes for Self-Direction 90
      - Attributes for Adaptable Measures 91

	Attributes for Defined Process	92
	Attributes for Foundation for a Continuous Process	93
	Attribute for Forward-looking View	94
	Attributes for Focus on the Critical Few	94
	Attributes for Integrated Management	95
	Attributes for Open Communication	96
	Attributes for Global Perspective	96
	Attributes for Teamwork	96
	Specific Procedures Employed	97
	Formats for Presenting Results	105
	Outcomes	105
	Resources Used	107
	Reliability and Validity	109
	Summary	110
<b>4.</b>	<b>Results</b>	<b>112</b>
	Data and Process Analysis	112
	Building the Tailored Methodology	112
	Expanding the OCTAVE Catalog of Practices	113
	Restructuring Data Collection	115
	Augmenting Threat Profile Content	118
	Restructuring Phase 3 Worksheets	119
	Review of Terminology	120
	Validation of the Tailored Methodology	121
	Testing in a K-12 School District	123
	Initial Meeting	124
	Guidance Session 1	125
	Guidance Session 2A	125
	Guidance Session 2B	128
	Guidance Session 3	129
	Review by K-12 School Representatives	132
	Findings	134
	Findings Specific to the Scarsdale Public School District	136
	SFG Review Findings	137
	K-12 Risk Methodology Structure and Use	138
	Summary of Results	139
<b>5.</b>	<b>Conclusion, Implications, Recommendations, and Summary</b>	<b>142</b>
	Conclusion	142
	Implications	144
	Recommendations	148
	Summary	151
	<b>Appendixes</b>	<b>156</b>
	A. Security Practices Unique to K-12	156
	B. K-12 Security Practices Consistent With OCTAVE Catalog of Practices	162

C. Mapping OCTAVE Principles to Attributes	170
D. Catalog of Practices for K-12 Risk Methodology	171
E. Table of Contents for K-12 Methodology Instructional Guidance	174
F. Current Educational Security Practices Survey Worksheet	177
G. Security Practices Summary	182
H. Protection Strategy for Educational Practices Worksheet	184
I. OCTAVE Criteria Principles to K-12 Risk Methodology	188
J. OCTAVE Criteria Attributes to K-12 Risk Methodology	190
K. Generic Threat Tree Example	193
L. Pilot Site Survey Responses	194
M. Abbreviations	200

**Reference List 205**

## Chapter 1

### Introduction

#### **Statement of the Problem Investigated and the Goal That Was Achieved**

How should school administrators establish and support appropriate educational access to the Internet? Reports issued by the United States (U.S.) Department of Education (ED) claim that two-thirds of the country's classrooms are now wired for Internet use (Kavanaugh-Brown, 2000). Estimates from the Federal Communications Commission (FCC) indicate that 90% of the public schools have some form of Internet access. According to Cattagni and Westat (2001), 60% are wired for individual classroom usage and other schools have shared computer labs and library media centers. Federal funding for this effort through the education rate (E-rate) program had reached \$5.8 billion as of February 28, 2001 (Cattagni & Westat).

#### *Technology Use in Education*

The role of technology in education is unclear. According to Holmes (1999), much of the classroom use of computers is custodial in nature. Students are given assignments unrelated to their studies to provide teachers with planning time while their students are occupied in the computer lab (Scott, 2001). According to Cuban (2001), who documented computer usage by shadowing students within selected schools in

California, a small cadre of early adopter teachers used technology extensively in the classroom, but for the majority of instruction, computer use was minimal. This same study identified a group of students (estimated at 5%) who gained technical expertise outside of the classroom and subsequently helped teachers and staff keep the technology functioning (Cuban). Based on a survey by the National School Boards Foundation (NSBF), students provided technical support in over half of the 811 school districts surveyed. Student technical assistance was reported as a critical resource to compensate for limitations in funding and availability of the school staff's technical skills (NSBF, 2002a).

Internet usage in K-12 schools and school districts is expected to grow as teachers gain familiarity with technology and the school curriculum is adjusted to include additional computer applications (Cattagni & Westat, 2001). The usage is expected to expand beyond simple topic searches to include e-mail, chat sessions, library subscription services, construction of Web sites, shared data and software files, videoconferencing, and virtual classroom experiences (WBEC, 2000).

### *Internet Context*

Convenience of access to an ever-expanding array of information and an extensive communication environment that supports direct links with networked devices on the Internet brings a unique suite of risks (Carpenter, 2001). The System Administration, Audit, Network, Security Institute (SANS), a provider of Internet security training, estimates that between 7,000 and 10,000 devices with known vulnerabilities are added to the Internet daily, and that hackers seeking these vulnerabilities are initiating thousands of programs on the Internet at all times (Landers,

2002). If such vulnerabilities are found and exploited, the information resources stored on networked devices could be corrupted and the contents damaged, lost, or copied illegally. Moreover, the control of the networked device can be usurped by internal and external sources for unexpected activities if proper protection mechanisms are not established (Schneier, 2000).

K-12 school administrators must recognize and address the risks inherent in the environment their systems have joined (Schneier, 2000). In a survey conducted in the spring of 2003 by the Computer Security Institute (CSI) and the San Francisco Federal Bureau of Investigation (FBI) Computer Intrusion Squad, 530 computer security practitioners working for U.S. corporations, government agencies, financial institutions, medical institutions, and universities were asked to report on security issues from the preceding 12 months. The summary results indicated that 95% detected computer security breaches, 38% detected network penetration from the outside, and 82% detected computer viruses (Richardson, 2003).

Systems are not delivered with sufficient levels of security to survive exposure on the Internet (Carpenter, 2001). Extensive lock-down procedures that include removing unneeded software, changing default passwords, incorporating anti-virus protection, and restricting administrative access for every device can improve the situation based on research of past exploits by the Software Engineering Institute (SEI) (Allen, 2001). These procedures are unique to the specific design of each device and require detailed knowledge of the specific hardware and software for successful application. As devices are linked into an infrastructure and connected to the Internet, protection of access to the

devices and control of individuals authorized to use them increasingly become areas of security concern (CERT, 1998).

Without proper controls, Internet connectivity can mean that every individual on the network from the source point to a target destination (e.g. Web site, e-mail recipient, chat room) can view and change all contents of any communication (Schneier, 2000). The addition of protection devices such as encrypted communication mechanisms are needed to assure the confidentiality and integrity of content (Parker, 1998). Protection for Internet-accessible devices against unexpected changes and unsafe content may require the addition of anti-virus software, firewalls, intrusion-detection capabilities, and filtering software (Lesniak, 2002). Controlling who can use the network and retrieve content from interconnected devices requires effective authentication and authorization mechanisms.

User access is commonly controlled through assigned identification codes and passwords. As a consequence, network users must choose passwords wisely and know how to protect their access capabilities (Parker, 1998). Added network switches and routers may be required to further limit which information assets a network user can access. Steps to maintain the integrity, confidentiality, and availability of network resources and communication content can be costly to implement and resource intensive to maintain (Allen, Alberts, Behrens, Laswell, & Wilson, 2000).

### *Risk for Children Using the Internet*

Content on the Internet is not subject to any review or rating system and adult-only material is widespread (Stein, 1999). The online pornography industry exceeded an annual level of \$1 billion by the end of 2000 (Lane III, 2000). SexTracker, a Web service

that monitors adult sites, issued reports of 26,000 active Web locations with as many as 60 million unique visitors a day (Webb, 2001). Filtering was proposed by software developers such as Microsoft and Netscape, and Internet Service Providers (ISPs), such as America Online (AOL), to screen out inappropriate material for minors (Hunter, 1999). However, Internet filtering has not been proved or disproved as effective in protecting children. Censorship opponents such as the Electronic Privacy Information Center (EPIC) and the American Library Association (ALA) claim the risk of unwarranted censorship exceeds the protection capabilities of available products (Hunter).

According to Stein (1999), regulations to control Internet advertising are not in place and, as a result, marketing companies are taking advantage of Internet connectivity mechanisms to bombard users of search engines and other Internet services with ads. Advertisers such as DoubleClick have developed techniques to exploit Internet connectivity and install hidden monitoring programs on user devices to track a user's Internet access. Prior Web site access is used to select content for banner ads and trigger the display of Web pages, called pop-up screens, which match perceived user interests (Scheer, 2001). Blocking mechanisms such as firewalls can be installed to restrict access to storage on a user's device and minimize the risk of this level of intrusion. Companies such as Lavasoft offer scanning software to locate these monitoring programs and deactivate them. However, the monitoring software can be reactivated by subsequent Web site access if blocking mechanisms are not implemented (Lavasoft, 2002).

Children with Internet access may communicate personal information inappropriately and illegally to outside organizations and individuals. Compliance with the

Children's Online Privacy Protection Act (COPPA) has added another level of complexity to the problem of managing Internet communications for schools with students under the age of 13 (Anthony & Cohn, 2000). This federal law was passed in 1998 and went into effect in April 2000 limiting, through regulations administered by the Federal Trade Commission (FTC), the online collection and use of personally identifiable information obtained from children under the age of 13 (FTC, 2003). Written parental permission is required for the collection and use of this data and strict privacy restrictions apply (Cannon, 2001). Children are easily tricked into providing information through games accessible at popular sites (Cannon). Information collection has become intense as businesses attempt to capture online the estimated \$200 billion in spending that children directly and indirectly influence through their families (Armstrong & Casement, 2000).

Even if the child provides no specific input, the use of electronic tracking and probes into the available data on an Internet-accessible device used by a child can be extensive if the device is not configured to block the monitoring (Armstrong & Casement, 2000).

Software tools are available on the Internet to track the physical location of an Internet-accessible device through information sent from that device within an Internet communication message. The National Center for Missing and Exploited Children in Alexandria, VA uses one such tool called VisualRoute from Visualware. This tool graphically displays the physical origins of communications to track threats against children and tips received at its Web site (Moad, 2001). The Google search engine, available to any Internet user at the Google Web site (<http://www.google.com>), provides an additional trace feature that returns a location map when a telephone number formatted

with hyphens is entered in the search request block. Any location with a listed telephone number is included in the mapping function. While VisualRoute and Google are not 100% accurate, the capability is sufficiently robust to place unsuspecting children at risk should someone seek to locate and harm them (Moad).

With Internet access, network users have the opportunity to violate copyright laws such as the Digital Millennium Copyright Act (DMCA) of 1998. It is a simple process to download popular music stored in Moving Picture Experts Group (MPEG) files that have an MP3 file extension (designating the file as audio) by using programs, such as Napster and Gnutella, that bypass copyright protection mechanisms (Clayton & Watkins, 2002). The ease with which tapes and CDs can be copied promotes a disregard for intellectual property rights (Colkin, 2002). Due to the popularity of free-music sites, the recording companies are striking back by filing lawsuits against ISPs that allow access to Internet sites where illegal copies of recordings are posted (Johnston, 2002). The Recording Industry Association of America (RIAA) initiated legal action against college students who provided free-music sites that violated copyright laws from college campus networks. These students bypassed acceptable use requirements and technology monitoring mechanisms that were established by the colleges and aimed to avoid inappropriate use of the connectivity. These cases were settled in May 2003 when the students involved in the suit agreed to pay between \$12,000 and \$17,500 each and cease illegal song-swapping (Reuters, 2003). These same issues can apply to software and other copyright materials that can be plagiarized easily with electronic tools. The RIAA has threatened to sue any identified sources of illegal music (Reuters). School administrators, teachers, and others who establish and maintain K-12 Internet

environments must consider ways to insure that users of the vast array of intellectual property housed on the Internet handle that content ethically (Armstrong & Casement, 2000).

Internet access can provide students and other network users with a means of violating the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001. An individual who attempts to access other Internet sites from K-12 facilities without authorization is subject to criminal prosecution, and the school or school district would be expected to assist in tracking the perpetrator (Mackenzie & Goldman, 2000). Police are reporting the involvement of youth in global crimes who do not recognize the magnitude of their actions (Snell, 2002). Since K-12 schools and school districts are actively encouraging students to build academic skills that would, ironically, also allow them to become hackers, careful consideration must be given to providing effective awareness education, deterrents, and monitoring mechanisms (Cuban, 2001).

#### *Risk for K-12 Schools and School Districts with Internet Access*

Information critical to the K-12 school or school district can be endangered by Internet access. For example, a Washington State high-school student broke into the school's computer system and altered transcripts for other students for a fee (Lange, Davis, Jaye, Erwin, Mullarney, Clarke, & Loesch, 2000). As K-12 schools and school districts expand the use of Web access and consider opening the use of networks to parents and community service groups, control of connectivity becomes more complex and the risk of illegal use expands (PTA, 2001). In a recent court case, a Philadelphia man was sent to prison for attacking a library Web site and posting obscene images

(Blackwell, 2002). Web sites can be extremely vulnerable to attack unless properly secured, and the existence of a Web site provides a footprint to the provider's network that may make the site easier to compromise (Scambray, McClure, & Kurtz, 2001).

Tracking intruders, determining how they gain access to a particular network, and coordinating activities between school administration and legal authorities for prosecuting hackers require time and technical expertise (Tipton & Krause, 2000). The flexibility of the Internet's communication mechanisms allows an attacker to adjust any and all communication content to avoid detection. As a result, tracking alleged perpetrators has become a global issue (Lipson, 2002).

Expanding network access to the Internet may also give unexpected participants undue access to personal information about students, staff, and faculty. Social security numbers, salaries, medical information, home addresses, grades, and other personal information may reside on the network (Allen et al., 2000). Restricting access to sensitive and confidential information by appropriate users requires careful consideration and monitoring to avoid the risk of privacy invasion, inappropriate modification, and identity theft (Parker, 1998).

Designing Internet connectivity appropriate to K-12 school or school district use is a challenge in security risk management; there are many options with no obvious right choice. The issues are both organizational and operational, and cannot be isolated to technology alone (Alberts & Dorofee, 2002). Every option has risks that must be identified, adjusted to specific local requirements, and appropriately managed (Schneier, 2000). Resources of time, money, and technical expertise are finite, so each school or school district must make choices among competing requirements (Allen et al., 2000).

By identifying the risks of each option, evaluating their potential impact, and prioritizing the risks, school administrators can transform risk assessment results into requirements that define policy and technology choices (Alberts & Dorofee). Applying a reusable process that structures the issues and incorporates good general security practices can facilitate the process of security improvement (Alberts & Dorofee, 2001a).

The Operationally Critical Threat, Asset, and Vulnerability Evaluation<sup>SM</sup> (OCTAVE<sup>®</sup>) Methodology was released for public use by the Carnegie Mellon<sup>®</sup> Software Engineering Institute (SEI<sup>SM</sup>) in September 2001 (Alberts & Dorofee, 2002). This methodology was developed to help organizations address operational security risk management, which includes the management of Internet connectivity in K-12 schools and school districts. The U.S. Department of Defense medical community selected this methodology to meet the mandated risk assessment requirement for compliance with Health Insurance Portability Accountability Act (HIPAA) security regulations (Alberts & Dorofee, 2001c). The methodology provides a systematic approach for a complex organization to identify the information assets that need protection, identify security requirements for these assets, identify potential threats, identify network vulnerabilities, and evaluate technology risks by comparing current practices to accepted best practices. The OCTAVE Catalog of Practices is incorporated into the OCTAVE Methodology to provide a basis of good security practices needed by all types of organizations (Alberts & Dorofee, 2001a). These practices are drawn from the analysis of Internet security problems reported to the Computer Emergency Response Team Coordination Center

---

<sup>SM</sup> Operationally Critical Threat, Asset, and Vulnerability Evaluation and SEI are service marks of Carnegie Mellon University.

<sup>®</sup> OCTAVE is registered in the U.S. Patent and Trademark Office.

(CERT<sup>®</sup>/CC), recommendations by the British Standards Institute (BSI) and the National Institute for Standards and Technology (NIST), and SEI experience assisting U.S. government and medical organizations with security risk management (Alberts, Dorofee & Allen, 2001).

The goal of this research was to validate the effectiveness of a security risk management approach tailored for the K-12 school domain. The OCTAVE Methodology was selected for use in this validation effort based on cost and tailoring capabilities. Through the use of tailoring capabilities within the OCTAVE Methodology, a domain-specific security risk methodology was developed for K-12 schools and school districts. This tailored methodology was validated at a selected school district and successfully applied by the school district. The selected K-12 school district included considerations of Internet security risk in its district planning to address technology support and improvement.

Design of the tailored methodology required identification of the unique information security issues appropriate to Internet connectivity for K-12 schools and school districts. Appropriate options were selected to tailor the OCTAVE Methodology to fit the unique needs of K-12 schools and school districts (Alberts & Dorofee, 2002). Validation of the methodology required personnel within a selected school district to learn and apply that methodology. An analysis team composed of five participants from the teaching, administration, and technology units was assembled to represent the range of technology needs and technical support throughout the school district. The analysis team discussed Internet security within a structured process that exposed participants to

the range of issues and good security practices that should be considered for use in a K-12 school or school district. The structured process guided the analysis team members in selecting appropriate protection strategies to meet the specific protection needs of their school district (Alberts & Dorofee).

Participants from the selected school district evaluated both the results of the methodology and the value of its use in addressing K-12 school security risk management. To be considered for selection, the K-12 school district was required to have a full age range of students and actively use technology within the curriculum at most grade levels. Technology support staff needed to work for the K-12 school or school district rather than an external provider organization to assure onsite availability and eliminate conflicts with vendor contract provisions. Analysis team participants were required to commit sufficient time to learn and complete the evaluation within an eight week timeframe.

The Scarsdale Public School District (SPSD) was the selected school district for validation of the tailored methodology. This K-12 school district met all the selection criteria. In addition, the curriculum director and technology manager expressed strong interest in identifying and addressing the security needs of the school district. The SPSP consists of one high-school with an enrollment of 1,200 students, one middle school with an enrollment of 900 students, and five elementary schools with enrollment in each school ranging from 350 to 500 students. Every school has at least one computer laboratory for use by every grade level. In addition to the laboratory, every classroom has active computer connections for instructional use by teachers. A fiber-optic Gigabit Ethernet wide-area network (WAN) interlinks all schools. The Technical Services staff,

with third-party support, coordinates district-based technology activities. ISP services, firewall operations, and content filtering are handled by a third party. Students attend regularly scheduled computer classes at all grade levels. The computer education curriculum includes courses addressing computer operations, publishing and presentation, creativity and design, problem-solving, and research. All students, starting in kindergarten, are provided with access to the school network.

Evaluation of the effectiveness of the K-12 tailored methodology at the SPSD was based on four perspectives. The first perspective was provided by Christopher Alberts, one of the researchers at the SEI who developed the OCTAVE Methodology. This review focused on the process of tailoring the methodology to maintain consistency with the OCTAVE Criteria (<http://www.cert.org/octave>), a set of general core requirements that must be incorporated into every tailored version (Alberts & Dorofee, 2001a). These requirements are described in detail in Chapter 3.

Participants at the SPSD, who provided the second perspective, reported an enhanced understanding of Internet security issues within the school district and perceived value for time spent using the methodology. Feedback from those participants also identified the need for additional changes to the tailored methodology. Those changes were compared to the OCTAVE Methodology to identify possible limitations in the initial tailoring of it and issues related to the effectiveness of using it in K-12 schools and school districts.

A third perspective from K-12 experts provided an indication of the applicability of the risk management approach to Internet security in K-12 schools and school districts beyond the selected school district. The tailored methodology was presented for review

and comment to a group composed of ten individuals actively participating in the K-12 school environment including school board members, technology directors, and superintendents. Review participants were selected from the membership of the Consortium for School Networking (CoSN), a national non-profit organization that draws its members from school districts and related organizations across the U.S.

The fourth perspective was assembled from observations of this researcher as the methodology was introduced to the selected school district and used by the analysis team. The resulting plans and strategies were expected to share commonalities with those from U.S. government agencies, financial institutions, universities, and foreign corporations that had already applied the OCTAVE Methodology. All organizations using Internet connectivity are impacted by security threats, such as worms and viruses, which place the integrity of network resources at risk (Pethia, 2003).

### **Relevance and Significance**

The use of Internet connectivity within K-12 schools and school districts touches a wide range of regulatory, political, and social challenges for educators (NSBF, 2002b). Regulations for educational reform to provide greater accountability, choice, and flexibility in federal programs were implemented in 2001 through the No Child Left Behind (NCLB) Act (ED, 2001). School districts such as Jefferson County, Kentucky (<http://www.jefferson.k12.ky.us>) assembled years of paper records into Web-accessible data repositories to help educators at local, district, state, and federal levels prove that the \$200 billion in federal spending initiated by the Elementary and Secondary Education

Act (ESEA) of 1965 provided benefit to children attending K-12 schools receiving these funds (ED). Funding through the Federal Communications Commission (FCC) E-rate program provided more than \$6 billion to establish Internet connectivity in K-12 schools, school districts, and classrooms as a portion of the ESEA funding (ED). To meet the NCLB requirements, educators must also prove that poverty, race, ethnicity, disability, and limited English proficiency have not hindered the progress of the children attending schools that received federal funds (ED).

Organizations such as the American Student List (ASL) and the National Research Center for College and University Admissions (NRCCUA) have deceptively collected information about children using survey instruments distributed in the classroom under the pretense of college scholarship opportunities and sold survey results to marketing organizations (EPIC, 2003). The 2001 Education Bill included a provision for parents to inspect survey instruments distributed in the classroom and exclude their children from participation (EPIC). According to the Electronic Privacy Information Center (EPIC), the ASL, NRCCUA, and other organizations that collect and sell information related to children might invoke the Freedom of Information Act (FOIA) to obtain access to data repositories assembled by K-12 schools and school districts to satisfy the NCLB reporting requirements. If K-12 schools and school districts do not implement appropriate information management, there is a high risk that parental restrictions will be bypassed and student privacy compromised (EPIC). Appropriate management of information access can be addressed through effective security risk management (Alberts & Dorofee, 2002).

## *Internet Content Filtering*

Federal legislators responded to concerns of voters attempting to protect children from seeing inappropriate Internet material with a series of laws including the Communications Decency Act (CDA) of 1996 and the Child Online Protection Act (COPA) of 1999. Censorship opponents such as the EPIC and the American Civil Liberties Union (ACLU) successfully challenged these laws in the courts as unconstitutional, based on the First Amendment freedom of speech (Hunter, 1999). In the court rulings that struck down the CDA and COPA, filtering was championed as a better alternative to federal legislation because it was less restrictive and designed to be equally effective (Hunter).

In 2000, supporters in the U.S. Congress favoring protective measures for children responded to the courts by passing the Children's Internet Protection Act (CIPA). This act linked a requirement for filtering Internet content to E-rate funding available for supporting Internet access for school-age children through the Telecommunications Act of 1996 (Klosek, 2000). The details of implementation including deciding when and how to apply filtering are the responsibility of each school district (Clark, 2001). In light of federal efforts to link public funding to a requirement for filtering, vendor hardware and software products were installed in K-12 schools and school districts across the country to restrict access to Internet content (PTA, 2001). The ALA and ACLU presented arguments before the Supreme Court in March 2003 that content filtering mandated by the CIPA blocks access to material that should be available to everyone based on constitutional protection and requested that the act be declared

unconstitutional. A decision on this issue is expected from the Court in 2004 (Pruitt, 2003).

Existing filtering products are highly controversial. None of the options work properly 100% of the time (EPIC, 1999b). A research team from Consumer Reports assembled a study test of the effectiveness of six filter products against 86 Web sites containing harmful content that filtering products should block. Their findings, described in the article titled "Digital Chaperones for Kids," published in *Consumer Reports*, March 2001, indicated the blocking process for all six products failed at least 20% of the tests (as cited in King, 2001). Without due care, the risks of exposure to illegal material and blocked access to legitimate sources are significant (Li, 2000).

The Supreme Court in *Reno v. ACLU* declared that the local community standard must be applied to define the line between pornography and obscenity. This line is critical since pornography is protected by the Constitution under the First Amendment freedom of speech but obscenity is not (Lane III, 2000). The determination of what is legal for adults and harmful to minors is subject to extensive local interpretation (Fienberg, 2001). A school would be criticized if a child saw inappropriate content, but held liable if anyone used school-provided Internet connectivity to gain access to illegal materials (Lane III).

The U.S. Congress identified the need for filtering to protect a child from unsuitable materials on the Internet and assigned the filtering responsibility to the parent or legal caregiver (GAO, 1998). A group of citizens in Holland, Michigan attempted to pass a referendum banning Internet access from library and school computers in their community because children might be exposed to "obscene, sexually explicit or other

material harmful to minors” (Bradsher, 2000, p. A12). The voters turned down the referendum with 55% opposed and 45% in favor; voter turnout was double the expected level. Exceptional voter turnout was attributed to the interest and concern of voters regarding this issue (Bradsher). Some caregivers are turning to home-schooling to maintain an assurance of quality and control over their child’s education. In 1999, over 850,000 children were schooled in their homes (Sale, 2002).

According to consumer research, only six percent of caregivers rely on filtering products at home when allowing children to be online without close adult supervision (King, 2001). In contrast, school technical support personnel rely primarily on content filtering to control access to the Internet (Cope & Brewin, 2000). A survey of technology decision makers in 811 school districts funded by the National School Boards Foundation (NSBF, 2002a) found that 90% of the respondents installed filtering software. In addition, 78% reported teacher supervision as the central part of their effort to provide a safe access environment (NSBF).

The application of content filtering requires two components: (1) a rating to be applied to each Internet address and (2) a filter module that uses the rating to determine whether to grant or block access to a site selection. Ratings can be assigned to a Web site through self-rating or via a third party. Also, ratings can be created dynamically within the filter module to block any content matching selected keywords that are considered objectionable (EPIC, 1999b).

The World Wide Web Consortium (W3C) developed an open standard called the Platform for Internet Content Selection (PICS) that provides a means for sites to incorporate a self-selected electronically readable rating within each Web page. The PICS

standard provides a universal language for Web site self-rating, establishes general rating-based rules, and defines a label format without providing guidance for the content of the label itself (<http://www.w3.org/PICS/iacwcv2.htm>). Rating systems have been developed by the Internet Content Rating Association (ICRA) (<http://www.icra.org>) and SafeSurf™ (<http://www.safesurf.com>) to provide a means for Web developers to implement the PICS standard (<http://www.safesurf.com/ssplan.htm>). However, self-rating is subject to both accidental and deliberate misinterpretation without penalty (Hunter, 1999).

The use of blocking software for the filtering module can allow the installer to select specific words that will trigger a browser to block a site irrespective of the site self-rating (EPIC, 1999b). Selecting word blocking can occur based on content in ads and banners appearing on pages that may be unrelated to the actual content of the page and vary with each access request. The installer must select whether to block unrated pages (EPIC). The filtering module can reside on a local device, an Internet access point at a school or school district network, an access point maintained by an ISP, a state-controlled Internet-access link, or a regional access point that crosses multiple states (Hunter, 1999). When installation choices apply to a wide geographic area, the potential for disagreement with local expectations is high, and the possibility of illegal access restrictions increases (ALA, 1999). In an effort to balance between competing views, the Bertelsmann Foundation released a proposal in September 1999 to establish a voluntary international content rating and filtering system, but that proposal did not gain wide acceptance (Hunter).

New York State leased a product called I-Gear (later renamed Web Security) from Symantec (<http://enterprisesecurity.symantic.com>) to filter Internet content for public schools in the state. Web site access was blocked by this product based on an encrypted list that identified sites considered unacceptable. Reverse engineering of this list by Peacefire, an advocacy organization for freedom of access to Internet information (<http://www.peacefire.org>), identified 470,000 sites that were blocked. According to Peacefire, 76% of the Web-based educational pages, or Web addresses ending in .edu, were blocked improperly, preventing school children from accessing educational information defined specifically for their use (Harrison, 2000). As K-12 schools and school districts become more reliant on Internet information sources, censorship opponents, such as ALA, ACLU, and EPIC, become more concerned about the ability of software filters to reflect value judgments by restricting access to selected Web content (Hunter, 1999).

Mechanisms for circumventing a filter are obtained easily using anonymous Web sites (e.g., <http://www.anonymizer.com>) or tools downloaded to a local device. Interaction with Web sites, e-mail, newsgroups, and chat groups can be hidden from the filtering module through encryption mechanisms (NSBF, 2002b). Other aids used to disable blocking software are provided by Peacefire, based on the organization's claim that much of the inappropriate blocking is deliberate and should be circumvented (<http://www.peacefire.org>).

Blocking software should inform the user of the blocking decision process so that inappropriate applications can be identified and corrected, but many software filtering packages do not provide this option (Balkin, Noveck, & Roosevelt, 1999). The installer

of the filtering module chooses how to inform the requestor about the filtering decision by blocking the full page or only blocking out the offending words. Filtering tools cannot evaluate words within a context or distinguish between different uses of a sequence of letters (Hunter, 1999). For instance, the Beaver College Web site disappeared from student availability after filtering software providers added “beaver” to their list of slang terms. As a consequence, the 147-year-old institution changed its name to Arcadia University (LaRue, 2000).

Typically, a third-party rating system is implemented using categories such as violence, profanity, sex, and nudity that are created by the rating group. Screening at the installation point is based on blocking some or all of the available categories. The rating group assigns a category to the Web locations identified as potentially objectionable. These assignments are stored in a proprietary database maintained by the rating group and used by the subscriber’s filtering module to apply the rating system (EPIC, 1999b). Software programs, employed by the rating group to search for new Internet sites that may warrant blocking, assign an automatic category based on a set of criteria developed uniquely by each rating group (Finkelstein, 2001). Researchers working for the rating group visually review the Web site to confirm or adjust the automatic selection to compensate for limitations in the automated process. Web locations are periodically rechecked for validity since Web content may change, requiring an adjustment to the category assignment. Changes and additions to the category assignment file are provided to subscribers on a predetermined frequency (Finkelstein).

Independent rating groups such as the United Federation of Child Safe Web Sites (UFCWS) offer a certification for filtering systems. The UFCWS provides the

iWatchDog™ program (<http://www.iwatchdog.info>) and certifies rating systems using the iWatchDog Commercial Certification Service (ICCS™). Any site using the ICCS™ certified rating system, such as SafeSurf™, can display a logo that indicates a guarantee of a child safety rating. Organizations voluntarily submit their Web site content to the iWatchdog™ program for review to obtain an approval rating (EPIC, 1999b). Filtering modules can be restricted to allow access to only certified sites or to limit access to a specific list assembled by a local user. This is considered the most restrictive approach in that only anticipated content can be viewed, and anything not on the accepted list is blocked (TechLearning, 2000).

All organizations are faced with risks stemming from the misuse of Internet connectivity and the subsequent access to inappropriate content (Cohen, 2000). The challenge in establishing access to the Internet is the inability to limit access to specific content areas deemed appropriate by the organization. Employee time and bandwidth are lost to entertainment opportunities for news, music, movies, and shopping (Cohen). Also, there is the potential to access controversial content (i.e., gambling and pornography) that carries legal restrictions in many geographic areas, as well as illegal content (i.e., obscene material and child pornography) (Lane III, 2000). In a survey conducted by the career Web site vault.com, 90.3% of the 1,200 U.S. employees who were contacted claimed to have accessed sites that were against their company's acceptable use policy (AUP) on company time (Cohen).

In response to potential liabilities, instead of trusting employees not to be tempted, many U.S. businesses, medical facilities, and government agencies implemented filtering programs to block employee access to inappropriate materials (Schulman, 2001).

Websense (<http://www.websense.com>) was the leading filter choice for U.S. businesses in 2002, based on sales dollars, installation locations that number over 18,000, and usage by the largest U.S. companies, including 282 of the Fortune 500 organizations (<http://www.websense.com/products/index.cfm>). According to the Websense Web site, the master database provides more than 80 possible category assignments for one billion Web pages with weekly updates for an additional 25,000. Category assignments are built manually, and the vendor offers a procedure for Web-page owners to dispute the category decision (Kranich, 2001). Available options allow for restrictions based on time of day, employee role, rating category, or keyword. Internet content and usage growth is estimated to double every year (Oklyzko, 2000). Maintaining an effective filter when the content base on the Internet is changing constantly requires a steady commitment of resources, and the potential for inappropriate blocking is high (Schulman).

### *Internet Risks Not Addressed by Content Filtering*

Cuban (2001) reports that selected students have advanced technological skills acquired outside of school through friends, family, and self-teaching. This competence has allowed these students to learn the details of their school's environment and to augment the administrative support of its technology infrastructure. Interviews with teenage hackers documented by Verton (2002) identify active learning of in-depth technology skills through exploration of home and school facilities by fifth-grade students ages 10 - 11. Some of these teenagers reported adjusting grades and plagiarizing assignments from other students by hacking into the school system. The students established prestige with peers, teachers, and administrators by creating school network problems they subsequently fixed.

Technically proficient parental and teacher authority figures helped some students learn to establish appropriate boundaries for acceptable and unacceptable actions and thereby avoid committing illegal acts (Verton, 2002). K-12 school and school district administrators must maintain a difficult balance between the educational role of the school environment to provide a learning space for children with a technology aptitude, and the business needs of the school environment to gather and protect information that must be kept private. K-12 schools and school districts have an added responsibility to provide technology use to all participants in the school environment based on commitments to E-rate and other connectivity funding sources (NSBF, 2002a).

Advanced technical skills are not always required for students to adjust online information inappropriately. A sixth grader took the opportunity to change his reading assignment grades after his teacher failed to close the computer session and then went to lunch (Shah, 2003). Six students at Fremont, California's Mission San Jose High School gained access to the student grading system and adjusted their semester grades by collecting the teacher's authentication data using keyboard-tracking software tools they obtained from the Internet and installed on the teacher's classroom computer (Akizuki, 2003).

Control through enforcement of AUPs can incorporate behavior expectations for all users of the school infrastructure (Littman, 1998). AUP implementation has been successful at the high-school and university level. However, an AUP is difficult to implement in an environment where participants are still learning reading and comprehension skills (Cattagni & Westat, 2001). Only 19% of the K-12 school districts included in a 2002 survey by the National School Boards Foundation (NSBF) have tried

to implement an AUP, and only 2% report any audit mechanism to confirm its effectiveness (NSBF, 2002a). An AUP codifies guidelines for online communication with specific sanctions for inappropriate use (Lange et al., 2000). In universities, AUPs may indicate that research activities cannot include commercial efforts (Lesniak, 2002). LeBaron and Collier (2001) contend that the AUP should reflect an overall policy for technology use at the school board level.

Writing an effective AUP is not an insignificant effort, and enforcement depends heavily on the appropriate wording and a consistent application (Kovacich, 1998). LeBaron and Collier (2001) suggest accessing Web sites that provide guidance for writing an AUP such as: Bellingham, Washington Board Policy (<http://www.bham.wednet.edu/policies.htm>); Armadillo at Rice University (<http://chico.rice.edu/armadillo/Rice/Resources/acceptable.html>); Internet Advocate (<http://www.monroe.lib.in.us/~lchampel/netadv.html>); and K-12 AUPs (<http://www.erhwon.com/k12aup>). Selecting an appropriate template must involve the consideration of how Internet content is used acceptably within the school's environment and connectivity issues that an AUP should address. Some AUPs are targeted to specific problems such as protection from pornography, while others focus on privacy issues (Chapin, 1999).

School administrators must consider whether the technology in place at their site supports the intent of their specific AUP. Parents may be required to provide permission in writing for their child's technology use based on the school's defined AUP (CoSN, 2002). Inconsistencies between the use of content-filtering software and school policy can be considered an inappropriate implementation of the AUP by the school and an

opening to liability if a child's Internet access is handled improperly (Anthony & Cohn, 2000).

In 2000, Mackenzie and Goldman reported that University of Delaware students launched hacker attacks into commercial enterprises in violation of the university's AUP. These attacks - at the time an internal policing issue for the university - are now in violation of the USA PATRIOT Act of 2001 (EFF, 2002). By providing the access means for illegal acts, a K-12 school or school district assumes part of the liability of the student's actions unless a clear pattern of definition and enforcement of acceptable use can be shown (Kenneally, 2002). University students throughout the world who have the access, skills, and time increasingly participate in attacks on other Internet users (EDUCAUSE, 2002). As the skills needed to execute attacks decrease, the risk of younger children's involvement in Internet abuse is expected to rise (Schwartau, 2001).

The amount of critical information about each child assembled at school Web locations is growing based on the recognition that caregiver involvement in the child's schooling is a key ingredient in student achievement and accountability (ED, 2001). Web site access provides an inexpensive and effective communication channel to link a child with parents and other individuals outside of the classroom environment who influence the child (ED, 2000a). Personal information about each child, such as a social security number, address, homework assignments, grades, and electronic report cards, can be accessed via the Web along with school calendars, school activities, and other general information (NSBF, 2002a). As more personal content for a child becomes remotely accessible, the risk increases that organizations and individuals such as peers, non-

custodial parents, advertisers, and pedophiles will attempt to use the content inappropriately (Quittner, 2001).

Computer access and the availability of Internet connectivity is expanding beyond the boundaries of the classroom for school children. For instance, two elementary schools in Pennsylvania participate in an experiment to provide 24/7 (24 hours a day, 7 days a week) connectivity aimed at proving the value of ubiquitous technology for education (O'Toole, 2002). In another experiment, fifth graders in Iowa schools are provided with a small handheld device for their individual use at all times (Levine, 2000). As school-provided access expands beyond classroom time, the teacher can no longer be expected to provide complete monitoring for Internet use. University administrators already experience many problems (such as the e-mail harassment of students and experimental hacking) that are attributed to expanded access to unrestricted Internet communication capabilities. These problems are expected to increase among younger students as unmonitored connectivity expands (Mackenzie & Goldman, 2000).

Universities report a growing struggle to balance open access with security management (EDUCAUSE, 2002). Faculty and administration in post-secondary schools have an increased awareness of security challenges and risks based on the national recognition of the technology capability available within this environment of high participant turnover, highly decentralized management, and broad technology diversity (EDUCAUSE). For example, in March 2003, a student at the University of Texas (UT) was charged with the largest information theft to date involving a university. In this case, the personal information of over 55,000 students, staff, and faculty was compromised using a security-access weakness that allowed a student to execute a program at the UT

Web site and retrieve data that the assigned authorization level should have blocked (Brulliard, 2003).

According to administrators at the University of Delaware, success in managing its networked environment requires an extensive emphasis on training students, faculty, and administration, coupled with enforced policies and practices that discourage abuse, assure the fair adjudication of offenders, and provide protection for victims (Mackenzie & Goldman, 2000). Programs such as Safeguarding the Wired Schoolhouse, funded through the Consortium for School Networking (CoSN, 2002), issue a similar message to K-12 schools and school districts - that the issues facing higher education are also a growing concern for younger students (CoSN).

Updegrave and Long (2001) in a presentation on March 19, 2001 to the EDUCAUSE/Internet2 Task Force on System Security identified six challenges for information security in higher education: (1) the tradition of freely sharing information; (2) limitations in direct control over individual participants; (3) a broadly disbursed technology environment; (4) limited financial resources already taxed to meet basic functional needs; (5) an extensive individual autonomy in defining and expanding available resources; and (6) a limited understanding of the role of centralized control on technology. Many of these challenges are applicable to K-12 schools and school districts as their technology environments expand. According to Updegrave and Long (p. 14), "K-12 school system networks are the only sites (in the U.S.) which have worse network and system security than higher education."

There is an expanding realization that any poorly protected site on the Internet is a potential threat to all Internet users ([http://www.cert.org/tech\\_tips/home\\_networks.html](http://www.cert.org/tech_tips/home_networks.html)).

Attackers can take control of unprotected devices and use them as remote staging areas for attacking others (Allen & Sledge, 2002). Negligence claims against the owners of insecure networks are proposed as a means of promoting responsible behavior by victims of hacker attacks (Kenneally, 2002). Responsible network management for every organization requires effective policies and procedures for managing acceptable use by network participants and sufficiently knowledgeable technical support to maintain the systems at a level where vulnerability exposure is minimized (Wadlow, 2000).

### *Security Risk Management*

Trust was a key component of the Internet design when it was implemented initially in 1969 (Schneier, 2000). Internet connectivity with cross-country linkages grew from four hosts distributed on four nodes in 1969 to 15 nodes and 23 hosts in 1971. The connectivity was used to facilitate communication among research and government sites (Zakon, 2003). The protocols established at that time such as the Border Gate Protocol (BGP), which allows routers to direct Internet traffic efficiently, were designed to scale easily and cheaply by building a communication environment using links among existing local area networks (LANs). Those links were based on an assumed level of trust that is no longer valid (Schneier).

The Computer Emergency Response Team Coordination Center (CERT/CC) was established in 1988 through a collaborative agreement between Carnegie Mellon and the U. S. Department of Defense. This agreement was established in response to the Morris worm, a self-replicating program released by William Morris that crippled the Internet earlier the same year and impacted worldwide communications (CERT, 1998). The

number of reported incidents of worms, viruses, and denial of service (DoS) attacks has risen from six in 1988 to 137,529 in 2003, doubling in volume each year (CERT, 2003a).

Analysis of incident data at CERT/CC indicates that shrinking levels of knowledge are needed to mount ever-expanding levels of attacks via the Internet (CERT, 2003b). Worm and virus attacks are spreading at an increasing speed and affecting a greater number of sites more rapidly. Reactive methods of protection are failing because software vendors cannot create and distribute patches ahead of the attack impact cycle (Staniford, Paxson, & Weaver, 2002).

The initial creator of a new attack process is highly skilled technically, but others with much less capability who learn of the exploit through electronic bulletin boards can easily adapt the code and reuse it against different targets (Parker, 1998). As communication capabilities on the Internet expand, the speed at which new attack information becomes available to less skilled agents increases (Allen, 2001). In its January 2003 report to the U.S. Congress, the Institute for Information Infrastructure Protection (I3P) included organized crime, terrorist groups, and citizens in foreign nations as being increasingly involved as major attack agents (I3P, 2003).

The ease of installation for Internet connectivity and the availability of standardized software tools from database vendors such as Microsoft and Apple to build Web access for existing data have lulled new users of technology into a false sense of security (Carpenter, 2001). The same tools that aid in building Web access are used in generating attacks (Scambray et al., 2001). The Google search engine, a widely used Internet tool available at the Google Web site (<http://www.google.com>), provides knowledgeable hackers with a list of unprotected Web-enabled databases that use

standard software templates when searches are initiated using default text phrases built into the templates (Null, 2003). Apple Corporation and the Drexel University College of Medicine were notified by Null when unprotected FileMaker Pro databases containing sensitive personal and medical information appeared in a search-query response contains phrases used by FileMaker Pro Web Companion, a component that provides Internet access to databases built using FileMaker Pro tools. Because of the low knowledge threshold and ease of use, tools such as FileMaker Pro are selected for use by K-12 schools and school districts (NETS, 2002).

Reactive protection strategies are insufficient due to the increased attack speed and severity (Allen, 2001). Vulnerability assessments are used by many organizations to identify and fix software security problems, but the results of those assessments are hampered because of limitations in the available assessment tools (Peltier, 2002). Vulnerability tools can identify patterns that match known problems in the technology infrastructure, but they cannot identify poor administration practices and missing or incomplete policies (Alberts, Behrens, Pethia & Wilson, 2000). Using vulnerability tools requires specialized technical skills, and the improper use of such tools can damage the technology infrastructure. The volume of output can be overwhelming and difficult to analyze. The recommended actions selected by these tools can be in opposition to the needs of the organization. Careful skilled review is needed before changes recommended by a tool are selected for implementation (Alberts & Dorofee, 2002).

Experience with the limitations of vulnerability assessments in providing sufficiently context-sensitive results led researchers at the Carnegie Mellon Software Engineering Institute (SEI) to develop a security risk management methodology that an

organization could self-direct and tailor to fit its specific needs (Alberts & Dorofee, 2002). A security risk management approach that includes both organizational and technological issues addresses a broader range of security risk than vulnerability assessments (Peltier, 2001). Security risk management emphasizes recognition, resistance, and recovery based on the premise that total avoidance is not feasible (Peltier). Each organization has a unique information environment and a finite level of resources with which to identify and establish controls in addressing security risk (Alberts & Dorofee). One of the major challenges in the security risk management field is the identification of relevant risk for a specific organization (Alberts et al., 2000). Each site has a unique network structure, a unique mix of technical capabilities, and a unique mix of network services and users. The Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) Methodology was released in September 2001 to address unique organizational security risk management needs (Alberts & Dorofee, 2001c).

The OCTAVE Methodology incorporates a Catalog of Practices (Alberts et al., 2001) that contains good security practices drawn from the analysis of problems reported to the Computer Emergency Response Team Coordination Center (CERT/CC), standards from internationally recognized organizations, and results from in-depth evaluations at medical, manufacturing, and government organizations (Alberts & Dorofee, 2001a). These practices represent good general security practices every organization should address to exhibit due diligence in handling security risk. However, detailed actions and domain-specific issues such as regulations and role-specific needs are not included in that catalog (Alberts et al.).

With the realization that organizations have neither unlimited resources nor unlimited time to devote to security risk management, each organization must select the appropriate security practice areas to mitigate based on its unique site characteristics, current operational environment, and applicable legal and regulatory mandates (Alberts & Dorofee, 2002). Instructions are provided within the OCTAVE Methodology for tailoring the processes and practices to address the needs of specific types of organizations (Alberts et al., 2001). OCTAVE tailoring capabilities were used in this investigation to incorporate unique security practices for K-12 schools and school districts into the methodology.

## **Barriers and Issues**

Designing and maintaining an appropriate and secure Internet connectivity solution that accommodates educational and legal requirements and is suitably flexible to handle the unique local needs of K-12 schools and school districts is a complex problem (Wasserman, 2000). Stakeholders such as teachers, librarians, students, parents, school board members, school administrators, and educational funding groups at local, state, and federal levels come from different disciplines with varying perspectives on security. Issues can be politically charged (Armstrong, Sibley, & Samara, 2003).

Accountability for the federal dollars spent on technology support for education is increasing without a clear definition of the expected role of technology in education (ED, 2001). Studies of the learning process, such as those conducted by the Archimedes Project at Stanford University's Center for the Study of Language and Information,

confirm the promise of technology to facilitate access to information, but indicate that access does not necessarily correlate to a better learning environment (Scott, 2001).

Teachers have been slow to adopt technology to enhance the educational experience, based on a survey of middle-school and high-school students by the Pew Internet and American Life Project in 2002 (Sarkar, 2002). Cuban (2001) identified the availability of technical assistance as a key ingredient for the expanded use of technology in the classroom. School administrators have focused on technology to help address existing resource constraints to meet administrative and regulatory responsibilities without recognizing the need for expanded resources to enhance the adoption of the new education medium (NSBF, 2002a). Federal programs and legislation such as the No Child Left Behind (NCLB) Act of 2001 increased the need for monitoring and reporting capabilities to meet the growing accountability focus of U.S. federal funding sources (ED, 2001). K-12 schools and school districts have responded by assembling online reporting facilities containing confidential and sensitive data (EPIC, 2003).

Controlling access to systems and services is more complicated in an environment with a transient population and heavily distributed management (Armstrong et al., 2003). Common practices used in business environments, such as individual access accounts with passwords and digital signatures, are more difficult to establish and maintain with a constantly changing population of young people (McNabb, Valdez, Nowakowski, & Hawkes, 1999). Closely monitored usage is recommended for very young students with progressive independence, as they prove able to act responsibly (Marcroft, 1998). The primary focus for monitoring online security has been the teacher, as reported by 78% of the 811 school administrators in the NSBF-sponsored 2002 survey (NSBF, 2002a).

Given the wide range of skills exhibited by teachers in the field of technology, the potential for inappropriate use of Internet access is high (NETS, 2002).

Technology support in the not-for-profit sector is difficult to obtain. Funding sources are inconsistent and often nonexistent (Schneider, 1999). The heavy reliance on volunteer support becomes an additional issue for school administrators (PTA, 2001). Students, teachers, and administrators may need to share network resources for cost-effective solutions (McNabb et al., 1999). When the available technical support cannot meet their minimum needs, K-12 schools and school districts supplement this support with student assistance (NSBF, 2002a). Teachers are urged to expand the use of technology with limited support and limited training (LeBaron & Collier, 2001). These same teachers are responsible for monitoring the appropriate use of technology by students (NSBF).

The expanded accountability imposed by NCLB regulations has motivated school officials in Maryland and Mississippi to seek assistance from industry volunteers such as AWS Convergence Technologies, Inc., which established a subsidiary company named OnTarget to provide a service that houses K-12 student data and provides reporting capabilities that meet NCLB requirements (AWS, 2002). Schools in these states input years of detailed student assessment information into databases that reside at corporate locations (Morgan, 2000). By using an environment for assembling and reporting sensitive data with which they have only a limited formal relationship, school officials risk alternative uses of that content without their knowledge (Alberts & Dorofee, 2002).

While many information protection strategies are available for addressing a wide range of specific Internet security issues, typically those strategies involve large financial

commitments, and the implementers are trained security professionals familiar with the intricacies of Internet communication (Parker, 1998). A low-cost methodology for information owners untrained in the details of information security to use to identify and address their own security risk is a recent development (Alberts & Dorofee, 2002). Released in September 2001, the OCTAVE Methodology is one of the first methodologies available for general use that can be tailored and self-directed by an organization without additional cost for training and support (Alberts & Dorofee, 2001c). Through the expanded application of the OCTAVE Methodology in its first year, the value of creating versions of the methodology unique to specific domains based on differences in organizational structure, regulatory climate, and risk exposure was confirmed (Alberts & Dorofee, 2002). Security practices within the OCTAVE Methodology are too general for domains with unique regulatory requirements (Alberts & Dorofee, 2001c).

Recognition of Internet security as a requirement within the K-12 school environment is relatively recent (CoSN, 2002). The primary focus at the national level is on accountability for the \$200 billion of federal money that was spent on technology for education since the passage of the Elementary and Secondary Education Act (ESEA) of 1965. The NCLB Act of 2001 is an extension of the ESEA with enforced accountability tied to standard test results (ED, 2001). The total cost of ownership is a major initiative of the U.S. Department of Education (ED) in understanding the full cost of technology including support, connectivity, replacement, disposal, retrofitting, and training (CoSN). Security is not included as a specific attribute in that program. Federal funding for security implementations is available at post-secondary institutions but not at K-12

schools and school districts at this time (Keith Krueger, personal communication, February 20, 2003).

### **Limitations and Delimitations of the Study**

This researcher has not attempted to address the value of technology in education. Many forms of technology have been applied to education over the years, and their success or failure must be based on the met or unmet needs of each school (Scott, 2001). The vision of how technology can be applied and the goals for using technology within the environment of student learning must already be established before an information security evaluation methodology can be used (ED, 2000a). This researcher has not addressed the definition of measurements for evaluating the penetration of technology into classroom use. Metrics such as classroom hours in the computer lab or assignments with computer-usage components were identified by Chambers, Lieberman, Parrish, Kaleba, Campen, and Stullich (2000) in a report commissioned by the U.S. Department of Education (ED), but the utility of such metrics has yet to be confirmed.

An appropriate Internet environment must support the learning goals and objectives defined by educators and not attempt to delineate a solution for educational problems with technology (Holmes, 1999). A general migration of education away from a teacher-centric focus to a student-centric one places a greater burden on K-12 schools and school districts for individualization (Hanson, 2001). Technology is identified as a low-cost way to meet this need, but the value of this transition is as yet unconfirmed (Norris, Solloway, & Sullivan, 2002). Researchers such as Healey (1998) identified problems caused by exposing children below a specified skill level to technology too

soon in their learning process. The concern that classroom time is consumed by devices when it should be focused on human interactions was not addressed by this research (Sabelli, 2001). Each school must establish the use of technology within the curricula selected for its students. A school's security issues must be considered subordinate to its learning goals. As such, the applicability of the technology must be determined before appropriate security controls can be defined (Healy).

The methodology used in this study addresses the planning aspects of information security and not the details of security monitoring and intrusion detection within an individual environment (Alberts & Dorofee, 2002). The OCTAVE Methodology provides a process for developing information security plans to protect critical information assets within a K-12 school or school district. Approaches to include evaluation results within a continuous planning cycle, as well as acquisition strategies for new technology, are suggested but not specifically incorporated within the OCTAVE Methodology (Alberts & Dorofee).

This researcher has not addressed a means of evaluating specific Internet content for value and accuracy. Internet connectivity offers access to valuable information as well as misinformation that is deliberately or accidentally misleading (Polly, 2001). Defining the line between appropriate controls and over-control must be handled by each individual K-12 school or school district. Within a range of behaviors, each K-12 school and school district establishes a level that is appropriate for the students, administration, teachers, parents, and others who are granted access to the local infrastructure based on local controls (CoSN, 2002).

Technology provides a means of establishing the standardized enforcement of selected security controls that apply equally to all participants. The OCTAVE Methodology provides a structured process for the identification of security risk to guide the selection of appropriate technology controls (Alberts & Dorofee, 2002). This process has neither defined the value of selected controls, nor identified a preference for centralized versus distributed control. Each K-12 school and school district must establish the level and manner of control appropriate to its needs before using the security risk methodology to identify inconsistencies that could allow the selected level of control to be subverted (Quittner, 2001).

This researcher has not tried to compare the value of different security risk assessment methodologies for K-12 schools and school districts. Rather, this researcher employs a methodology that is widely used, available at no cost, and capable of incorporating the context-sensitive issues unique to a domain such as K-12 schools and school districts. In addition, the methodology selected for this research is specifically identified not to promote or reject specific technology standards, equipment, or connections since K-12 schools and school districts use a wide range of devices and connectivity solutions (Cattagni & Westat, 2001). Prior to defining information risk, each entity must define the hardware and software environment that best fits its needs within the regulatory and financial limitations imposed on it both internally and externally (Alberts & Dorofee, 2002).

## Definitions

*Asset* – Something of value to the entity such as information, systems, services, and people. An asset is considered *critical* if its inappropriate disclosure or modification, unavailability, or destruction would prevent the K-12 school or school district from fulfilling its mission (Alberts & Dorofee, 2002).

*Availability* – The period of time or frequency that an asset is present or usable (Alberts & Dorofee, 2002).

*Best Practices* – Security practices identified by security experts as effective in addressing Internet security risk (Parker, 1998).

*Confidentiality* – The need to keep information that is private, sensitive, personal, and proprietary inaccessible to unauthorized users (Alberts & Dorofee, 2002).

*Evaluation Criteria* – A measurement of risk to the K-12 school or school district as expressed through a set of negative occurrences that could happen and the qualitative degree (high, medium, or low) to which an occurrence will impact the mission and continued existence of the entity (Alberts & Dorofee, 2002).

*Exploit* – The use of technology to violate security policies established to protect critical information assets (Peltier, 2001).

*Filtering Module* – Software or hardware that prevents access to certain Internet sites or Web content based on assigned criteria (EPIC, 1999a).

*Generic Threat Profile* – Based on SEI experience with threat analysis, a general set of threat profiles developed to apply to a wide range of organizations. These profiles group threats into four categories: (1) human actors using network access; (2)

human actors using physical access; (3) system problems; and (4) other problems (Alberts & Dorofee, 2002).

*Information Assurance* – Protection of the data available within a networked environment to provide a specified level of availability, integrity, confidentiality, and authenticity (McKnight, 2002).

*Integrity* – Validity and wholeness of an information asset (Alberts & Dorofee, 2002).

*OCTAVE Approach* – A framework that incorporates aspects of organizational management, risk management, and information security risk evaluation for application to security risk management (Alberts & Dorofee, 2001a).

*OCTAVE Catalog of Practices* – Good general security practices for strategic and operational security areas drawn from the analysis of security problems reported to the CERT/CC, the SEI's experience in security risk evaluations, and security practice standards from the British Standards Institute (BSI) and NIST (Alberts & Dorofee, 2002).

*OCTAVE Criteria* – Key concepts referred to as principles, characteristics of the key concepts referred to as attributes, and defined results referred to as outputs that define the requirements for a methodology that supports the paradigm for security risk management defined in the OCTAVE Approach (Alberts & Dorofee, 2001a).

*OCTAVE Methodology* – A three-phase process that is based on the OCTAVE Approach and used to apply risk management to information security through the identification and analysis of information assets, threats, and vulnerabilities within organizational and technological infrastructures. The OCTAVE

Methodology supports the development of plans for improving the security of identified assets based on good security practices (Alberts & Dorofee, 2001c).

*Rating System* – Criteria used by a vendor to assign Internet sites to categories for access blocking through the use of a filtering module (EPIC, 1999a).

*Risk* – A threat with an associated impact. Risk involves a triggering event that may be initiated by a human, technology, or natural causes. That event will impact an information asset, but whether or not the event will occur is unknown (Alberts & Dorofee, 2002). The severity of each risk varies for each organization based on its selected risk evaluation criteria (Peltier, 2001).

*Security Practices* – Actions initiated by an organization that help implement and maintain security (Alberts & Dorofee, 2002).

*Security Requirements* – Qualities of an asset (e.g., confidentiality, availability, and integrity) that are important for the organization to protect. Failure of a security requirement results in a security compromise outcome (disclosure, modification, loss/destruction, or interruption) (Parker, 1998).

*Technology Vulnerability* – Weakness in the infrastructure that allows an asset to be compromised. Technology vulnerabilities are introduced through the application design, implementation, and configuration of the network infrastructure (Alberts & Dorofee, 2002).

*Threat* – The potential for an occurrence of an undesirable event that would compromise the security requirements for an asset (Alberts & Dorofee, 2002).

*Threat Profile* – A visual depiction of the sources of a threat to an information asset composed of an access means (network access, physical access, system problems, or other problems); an optional actor (insider or outsider); an optional motive (accidental or deliberate); and a security compromise outcome (disclosure, modification, loss/destruction, or interruption) (Alberts & Dorofee, 2002).

*Vulnerability Assessment* – An evaluation of a network infrastructure and/or selected components such as servers, desktop computers, firewalls, and routers. A vulnerability assessment employs software tools written to identify known security problems based on missing software patches; default configuration options; and other design, configuration, and implementation errors that allow intruders to compromise the device or infrastructure (Peltier, 2001).

## **Summary**

The expanded use of Internet connectivity in K-12 schools and school districts provides access to a vast array of content and enhances communication capabilities that may improve teaching and administration (PTA, 2001). Extensive resources through programs such as E-rate were applied to connect schools with the Internet (ED, 2001). Content filtering is mandated for Internet connectivity supported by E-rate funds (ED), but the value of filtering remains controversial (Hunter, 1999). Court challenges have been successful in removing requirements imposed by the Communication Decency Act (CDA) and the Child Online Protection Act (COPA), and a similar fate is expected for those imposed by the Children's Internet Protection Act (CIPA) in 2004 by the Supreme

Court (Pruitt, 2003). Extensive resources were applied to insert Internet connectivity into the K-12 school environment. However, issues related to the security of K-12 Web connections, network resources, and safeguarding users from access to materials deemed inappropriate did not receive an equivalent level of attention (NSBF, 2002a).

Teachers with limited technical training and limited technical support are required to address a wide range of technical needs for the K-12 schools and school districts (NSBF, 2002a). Students with access to technology outside of the classroom both challenge and assist the capability of teachers, and gain broad access to school technology resources that may not be sufficiently supervised (Schwartau, 2001).

Efforts by K-12 schools and school districts to address the accountability requirements of student performance imposed by the No Child Left Behind (NCLB) Act of 2001 through the construction of data repositories have expanded the volume of personal student information available via the Web (AWS, 2002). The protection mechanisms applied to this sensitive information appear insufficient (Allen, 2001).

Risks to information assets from Internet access have multiplied, options for attacking Web-based information assets have expanded, and the technical expertise needed to inflict great damage using Internet connectivity has rapidly decreased (Schneier, 2000). Each K-12 school and school district has a unique set of technology requirements, participants, and infrastructure that define potential security threats within its environment (Alberts & Dorofee, 2002). Also, each K-12 school and school district has a different level of risk tolerance based on the potential impacts a realized threat would deliver. Identifying the threats, risks, unacceptable impacts, and ways of

effectively applying protection is best accomplished through information security risk management (Peltier, 2001).

The OCTAVE Methodology, a three-phase approach to information security risk management, has been applied successfully in over 1,000 medical, government, financial, and manufacturing organizations throughout the world (Alberts & Dorofee, 2002). The OCTAVE Methodology provides a suitable framework for addressing security risk in K-12 schools and school districts. This methodology is a self-directed process that incorporates good general security practices with tailoring mechanisms for addressing unique security needs (Alberts & Dorofee). This researcher identified the unique security practices and issues appropriate to K-12 schools and school districts. Those unique needs were applied to the OCTAVE Methodology to develop a tailored security risk methodology. The Scarsdale Public School District used that methodology to address its security risk management needs.

## Chapter 2

### Review of the Literature

#### **Historical Overview of the Research Literature**

Three streams of research converge to establish the basis for using security risk management for the protection of Internet connectivity in K-12 schools and school districts. One stream centers on research into the actual uses of technology within K-12 schools and school districts, and the perceived value of infusing technology into education. The identification and response to perceived problems arising from the use of the Internet by K-12 students form a second stream. This second stream is interlinked to the growth of access to pornography, gambling, and other adult-only content, as well as ready access to undesirable elements that prey on the unsuspecting via the World Wide Web. The third stream is built on research stemming from the recognition by medical, financial, and government organizations of the need for information security risk management to balance the expanding reliance on Internet connectivity with the growing risks connectivity introduces. Each stream has a wealth of research literature that, when blended together, establishes a critical need for security risk management within K-12 schools and school districts.

### *Use of Technology in Schools*

The establishment of the E-rate provided a major funding source for inserting technology into the K-12 classroom (ED, 2000b). Preliminary surveys commissioned through the U.S. Department of Education (ED) identified this infusion as a success based on the growth of Internet access in the K-12 classroom from 1994 to 2000 (Cattagni & Westat, 2001). A large portion of E-rate funding was targeted to support K-12 schools and school districts in less financially capable regions, and to address the perceived digital divide assumed to exist between the affluent and poor geographic regions (ED, 2000b). An ED study released in 2000 indicated that the geographic areas evaluated with the highest level of poverty had the lowest percentage of application requests for available E-rate funding.

### Measuring Technology Value

The Web-Based Education Commission (WBEC), in a report to the U.S. President and the U.S. Congress in December 2000, predicted that computer usage would have a direct and positive impact on student learning, and underscored the need for expanded teacher technology training and research in the application of learning tools in K-12 schools and school districts (WBEC). Another study performed by Norris, Soloway, and Sullivan (2002) considered the impact of technology over the last 25 years on a range of possible effects on student performance, including higher test scores and increased student motivation. Study results indicate a negligible impact so far, and the authors claim that the potential impact will not be realized until technology is as readily available to the student as the textbook (Norris et al.). On average, nine children share each computer in K-12 schools in the U.S. (NSBF, 2002a).

Research reported by Armstrong and Casement (2000) identified two assumptions that form the basis for emphasizing technology in K-12 schools and school districts. The first is that computer technology makes education more productive, relevant, and interesting for all students. Based on that assumption, the installation of any technology facilitates student learning (Armstrong & Casement). The second assumption is that if children are to fully participate in a society that is increasingly dependent on technology, schools must teach them about that technology. LeBaron and Collier (2001) assembled a set of success stories on the benefits of infusing technology into the classroom. Since most of the examples they cite occurred in 2000 and 2001, it is too soon to evaluate the long-range impact of technology availability and use on student learning. Kallick and Wilson (2001) attempted to define a way to measure the value of technology within the K-12 classroom by identifying changes within the school environment. Those changes included planning approaches for technology use and specific assignments that use multimedia capable of providing added value to the learning process. However, the success of that attempt is unconfirmed except by individual comments from teachers and students.

A study by Cuban (2001) involved an in-depth review of technology usage in three California K-12 schools. The results were evaluated based on the characteristics of the student and teaching populations of each school. Cuban sought to identify a correlation between economic levels and years of experience, or some other indicator of teacher motivation in support of technology adoption. According to Cuban, the primary indicators that motivated technology adoption were administrative support provided in

the form of recognition, the allocation of additional time for teacher skill building, and the availability of skilled technical resources for problem resolution.

The U.S. Department of Education (ED) identified a greater availability of technology in schools, the effective usage of technology by teachers in the classroom, and student's increased technology literacy as emerging priorities in 1996 at the Forum on the Future of Technology in Education (ED, 1997). The International Society for Technology in Education (ISTE) established qualitative standards of excellence for K-12 schools and school districts. Based on those standards, the ISTE defined strategic goals for the effective use of technology by administrators, teachers, and students in the National Education Technology Standards for School Administrators (NETS-A), National Education Technology Standards for School Teachers (NETS-T), and National Education Technology Standards for School Students (NETS-S) (ISTE, 2002). The Consortium for Technology Standards for School Administrators (TSSA) has contributed strategic planning approaches to technology with an emphasis on the added value technology brings to administration (TSSA, 2001).

The ISTE and TSSA emphasize the quality and benefits of technology. However, few metrics exist with which to compare the value of the technology-enhanced classroom approach to the traditional classroom approach. Norris, Soloway, and Sullivan (2002), using brief survey questionnaires administered to 10,000 teachers over a range of five years, compared the application of technology in the classroom to state and district achievement test results for the students exposed to the technology. No significant impact from technology use has been achieved so far (Norris et al.). Technology infusion into the classroom has been attempted in the past with television broadcasts, cable

programming, and video projection. According to LeBaron and Collier (2001), much of this equipment remains unused with no impact on classroom learning. Without clear value, teachers will likely view the process associated with deploying technology and transiting from one media to another for curriculum delivery in the classroom as time-consuming and costly and therefore resist it (LeBaron & Collier).

Fisher (2000) suggests that a technology tools that provides content manipulation and deconstruction (such as zooming, stop-action, repositioning, and moving images) adds value to the teaching capabilities because it allows each student to manipulate curriculum content for individual learning. Potentially, each child will have a preferred media for learning just as individuals have a preferred communication style (Armstrong & Casement, 2000). Kallick and Wilson (2001) do not think that specific technology characteristics have intrinsic educational value because the tools for content manipulation and deconstruction are changing too quickly to be analyzed effectively. According to Kallick and Wilson, the successful adoption of technology in the classroom depends on individual teacher acceptance within the existing course content and budget planning mechanisms. Further decomposition of the technology's potential uses does not increase its educational value (Kallick and Wilson).

### Legislative Mandates

K-12 schools and school districts must adhere to the regulations issued by local, state, and federal agencies to assure accountability and standardization in educational practices. The range of regulations that apply to each K-12 school and school district can differ based on the types of additional services provided to the students (such as health care and psychological counseling) and the level of access to course materials granted to

students and teachers (Salomon, Cassat, & Thibeau, 2003). Regulations that apply to most K-12 schools and school districts are described in the remainder of this section.

The No Child Left Behind (NCLB) Act of 2001 establishes measurements for the accountability of the local and state decision-making processes in providing assistance to disabled and under-served children, including the homeless and those who live in the inner city. Local and state officials must assure that all K-12 schools meet or exceed statewide proficiency goals (ED, 2001). Children served in unsafe or poorly performing schools can transfer to another school with the help of federal funds. A school losing a significant portion of its student body through this transfer mechanism will close (ED).

The Family Educational Rights and Privacy Act (FERPA) mandated protection for the privacy of student's educational records (ED, 2002a). Parents have the right to inspect their children's school records and request corrections, and children who turn 18 can inspect and correct their own records. Written permission is required from the parent or child over 18 to release student school information to parties not specifically exempted. Exempted requests would originate from school officials with legitimate educational requirements, another school to which the student is transferring, financial aid providers, and emergency health care providers (ED). Directory information consisting of student's name, address, telephone number, date and place of birth, honors, awards, and dates of attendance may be released without consent, but the parent or child over 18 must be notified in advance and provided with an option to be removed from the directory (ED). Advertisers and other mass-mailing organizations request directory information from educational institutions under the Freedom of Information Act (FOIA) for use in targeted solicitations (Saloman, Casset, & Thibeau, 2003).

The Electronic Privacy Information Center (EPIC) (<http://www.epic.org>) presented arguments to the U.S. Supreme Court in January 2003 through a brief filed in a FOIA case (*BATR v. City of Chicago*). The EPIC claims that technology can allow broad, open access and public oversight to government information if that technology is applied appropriately to protect private data. The EPIC is joined by 16 legal scholars and technical experts in advocating the use of technology to encode personal data instead of removing it before responding to FOIA requests. If the Court agrees, information providers will no longer be responsible for limiting access to private data, but will be required to apply the data-encoding technology needed to restrict access (Pruitt, 2003). K-12 schools and school districts that collect personal student data need to evaluate the mechanisms currently in place to meet FERPA regulations and consider how those mechanisms may be impacted by future changes in regulations (Pruitt).

The Health Insurance Portability and Accountability Act (HIPAA) of 1996 was enacted to protect the privacy of patient's medical data. K-12 schools and school districts that participate in the health care of students and teachers may be obligated to comply with the specific mandates of the privacy and security regulations within the HIPAA issued by the U.S. Department of Health and Human Services (DHHS) (Salomon et al., 2003). Entities subject to HIPAA regulations were required to provide written notice of electronic information practices to all participants by April 14, 2003. To assure compliance, these practices must include manual or technology-based mechanisms that monitor and confirm the protection of health information within the entity (Salomon et al.).

California voters approved regulations that apply to all entities collecting personal information about California residents. Those regulations mandate individual notification when personal information is subjected to inappropriate disclosure. Other states are expected to follow this lead (Salomon et al., 2003). An education reporter in Palo Alto, California was able to access student's grades, phone numbers, addresses, medical information, psychological evaluations, and photographs using the Palo Alto Unified School District's insecure wireless network (Metz, 2003). This problem was later addressed by the district superintendent, but not before there was adverse publicity and threats of legal action from parents who had not been notified of the disclosure (Metz).

K-12 schools and school districts that work closely with colleges and universities are impacted by the Technology Education and Copyright Harmonization (TEACH) Act of 2001 (Salomon et al., 2003). This law relaxed certain copyright restrictions to provide a broader use of materials within the framework of technology-mediated educational settings. Unauthorized retransmission is strictly prohibited, and technology controls for authentication and access protection are required (Salomon et al.).

There is a growing reliance on technology to enforce federal school regulations. Without effective management, limitations in the technology expertise in K-12 schools and school districts will increase the risk of regulatory noncompliance (Salomon et al., 2003).

### *Protection for Children Using the Internet*

Early studies by Stein (1999) pointed out that increased computer usage by children of K-12 school age reduced the number of hours children spent in front of the television. Parental concern for children's use of the Internet to access inappropriate

content was accelerated by warning reports issued by the U.S. Federal Bureau of Investigation (FBI) (1998) and federal committees such as the Committee on Commerce, Science, and Transportation (GAO, 1998). The visibility and profitability of the pornography industry rely on the strong communication capability of the Internet based on documentation by Lane III (2000). Regulations such as the Communications Decency Act (CDA) of 1996 and the Child Online Protection Act (COPA) of 1999 were passed to mandate the behaviors of Web site providers for handling content inappropriate for children. The constitutionality of the mandates was successfully challenged in the courts as violations of the First Amendment by censorship opponents such as the EPIC and ALA (Biskupic, 1999). The U.S. Congress shifted the regulatory effort to the K-12 schools and school districts by linking Internet access supported through E-rate funds with a filtering mandate to protect each child from accessing unsuitable materials on the Internet (ED, 2000b). As a result, each K-12 school and school district that implemented connectivity funded by the Child Internet Protection Act (CIPA) through the E-rate program was required to implement content filtering before July 2002 (ED).

A study by Neumann and Weinstein (1999) pointed out that every parent has a unique definition of what is harmful to a minor based on individual beliefs and no single definition can be successfully applied by a central authority. Content filtering should allow for parental involvement in the guidance role, but no regulation currently supports this recommendation. There is no clear agreement on what is harmful to minors (Neumann & Weinstein).

Filtering opponents such as the EPIC launched a series of studies identifying the major faults of available filtering products (EPIC, 1999a). The National Coalition

Against Censorship (NCAC) published a public policy report by Heins and Cho (2001) analyzing available content-blocking products, and all were identified as performing inappropriately depending on the selected test sites. On May 31, 2002, a three-judge panel in Philadelphia ruled that the CIPA was in violation of the First Amendment. An appeal was granted for U.S. Supreme Court review, but the response of the Court is unknown at this time (EPIC, 2002).

The extensive increase in unwanted e-mail generally containing references to pornography, illicit pharmaceuticals, physical-enhancement procedures, sweepstakes, and other topics inappropriate for children is regarded as a major problem by Symantec Corporation, an Internet security provider (Symantec, 2003). Symantec funded a survey conducted by Applied Research to identify children's responses to inappropriate e-mail content. In this survey, 1,000 children between the ages of seven and 18 were interviewed to determine the extent to which they are subjected to unsolicited e-mail and their response to those intrusions (Symantec). Over 80% of the children using e-mail reported receiving inappropriate content daily, and 46% responded that they gave their personal e-mail addresses to unfamiliar Web sites or strangers without their parents' consent (Symantec). When the child is under 13 years of age, both acts are in violation of the Children's Online Privacy Protection Act (COPPA). K-12 schools and school districts must consider the accountability issues for inappropriate actions by Web sites when school-provided connectivity is used as the access mechanism (Anthony & Cohn, 2000).

A study by Verton (2002) identified children with advanced technical skills as a growing risk to other Internet users. Much of the available research is anecdotal and

obtained through interviews with convicted juvenile hackers. However, technical analysts at the SEI have confirmed the ready availability of technical tools that can be used for broad Internet attacks with limited technical skill (Pethia, 2003). The growing technical capability of children with unsupervised access to technology presents an increasing potential to create Web-based problems (Carpenter, 2001).

One incident at the Newark Junior High School in New Jersey involved a seventh grader who hacked into the school system and deleted grade files for ten of the 55 teachers, resulting in a two-day delay in home progress reports (Kuznia, 2003). The impacted teachers blamed the lax technical security on recent budget cuts in technology support (Kuznia). In a separate incident, a junior at the Marion High School near Rochester, New York deleted all the password-protected student folders where class projects were stored (Legon, 2003). The student in New Jersey was expelled, and the student in New York was arraigned on felony charges. In yet another incident, a student at Richard Middle School in Richland Hills, Texas sent an e-mail to every computer in the school using an obscure system utility. Teachers determined that use of that utility constituted unacceptable use even though no acceptable use policy (AUP) was in place and the student was suspended for three days (Lieber 2004).

### *Security Risk Management and the OCTAVE Approach*

The transition from stand-alone computers to networked environments increased the importance of protecting the information accessible through the Internet (Lange et al., 2000). Scambray, McClure, and Kurtz (2001) provide a comprehensive reference to techniques and mechanics used to create Web-based security problems. Most of the attacks are software specific and tied to selected operating systems, browsers, computer

software development languages, and communication enablers such as e-mail and chat software (Allen, 2001). Protection requires an in-depth assessment and adjustment of purchased systems to remove security weaknesses that are often provided by a vendor to allow for ease of installation instead of secure functioning (Allen). Extensive technical knowledge of the specific hardware and software tools used in the construction and support of each network component is required to establish a secure infrastructure (Allen). Detailed steps, also called security practices, are provided by organizations such as CERT/CC and Mitre Corporation that research Internet vulnerabilities to help the installer minimize the likelihood and impact of technical attacks (Wadlow, 2000). Standards for information technology security practices, such as ISO 17799, are published by the International Standards Organization (ISO).

In addition to techniques for the secure installation of selected hardware and software, specific protection tools are available that focus exclusively on network security. Encryption techniques, firewalls, and intrusion-detection tools address a range of technical protection requirements such as the confidentiality of information during transmission, the rejection of transmitted information that matches known vulnerability patterns, and the identification of potentially inappropriate network access (Stallings, 2000). Each added security function requires special technical skills as well as additional financial resources to evaluate and implement it. Organizations with finite resources for technology, such as educational institutions, are faced with a difficult choice between added functional capabilities and security protection (Updegrove & Long, 2001).

Defining appropriate protection requires the identification of potential risks to information assets in the infrastructure and the ensuing impact should the risk be realized

(Peltier, 2001). Many security risks, such as password management and policy enforcement, materialize through the organizational use of network capabilities and are outside of the direct control of the technicians (Parker, 1998). Educational institutions that do not regard technology as part of the primary organizational mission may not have a standard mechanism for addressing organizational security issues (Alberts & Dorofee, 2002). An information gap exists between the technical staff who react to the infrastructure security problems and organizational managers who focus on the expanding information needs of the organization (Stoneburner, Goguen, & Feringa, 2001). Organizational managers are slow to realize their responsibility for provisioning information security due in part to a lack of recognition of the reliance level the organization has on technology (Lipson & Fisher, 1999).

The gap between the organizational perspective and the technological perspective of security was recognized by researchers within the continuous risk management program at the SEI (Alberts et al., 2000). A need existed for a proactive organizational approach to defining and addressing security risk by blending the perspectives of multiple levels of the organization. That need was met through the design of a security risk management framework that relied on a cross-functional team to identify, analyze, plan, track, and control risks within acceptable levels (Alberts et al.). The experience and techniques from SEI research in project risk management were applied to security risk, leading to the development of the Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) Methodology. That methodology addressed the identification, analysis, and planning needs for security risk management (Alberts & Dorofee, 2002).

SEI researchers Christopher Alberts and Audrey Dorofee developed the OCTAVE Methodology and produced a technical report (Alberts & Dorofee, 2001a) that summarized the aspects of organizational management, risk management, and information security risk evaluation that were incorporated into the OCTAVE Approach design framework. The OCTAVE Methodology is a security risk management methodology designed using the OCTAVE Approach and tailored specifically for large medical and government organizations (Alberts & Dorofee, 2002). Other tailored security risk management methodologies can be constructed using the OCTAVE Approach as long as the tailoring guidelines, referred to as the OCTAVE Criteria, are applied (Alberts & Dorofee).

OCTAVE Methodology activities are focused on the planning portion of the risk mitigation effort to establish a communication mechanism across the organization and to formalize a means for recognizing and addressing security risk (Alberts & Dorofee, 2002). Once the plan is defined using the OCTAVE Methodology, the organization will need to implement, monitor, and control the specific elements within the plan, and subsequently adjust the plan based on its effectiveness (Alberts & Dorofee). These additional requirements are not part of the methodology, but are necessary for the organization to benefit from the planning effort. Figure 1 provides a diagram of the sequence of steps needed to implement security risk management within an organization, highlighting those addressed through the application of the OCTAVE Approach (Alberts & Dorofee).

In applying the OCTAVE Methodology, or another tailored version of the OCTAVE Approach, an organization addresses the Identify and Analyze steps, and initiates the Plan step of security risk management.

- *Identify* – Capture organizational information assets and related security requirements, capture organizational and technological threats to information assets, and compare current organizational protection strategies to best practices.
- *Analyze* – Define organizational impact criteria, evaluate risks to information assets, and prioritize risks based on the level of their impact on the organization.
- *Plan* – Develop risk mitigation plans to protect critical information assets, action plans to address critical weaknesses in the technology infrastructure, and a protection strategy to address broad organizational risks.

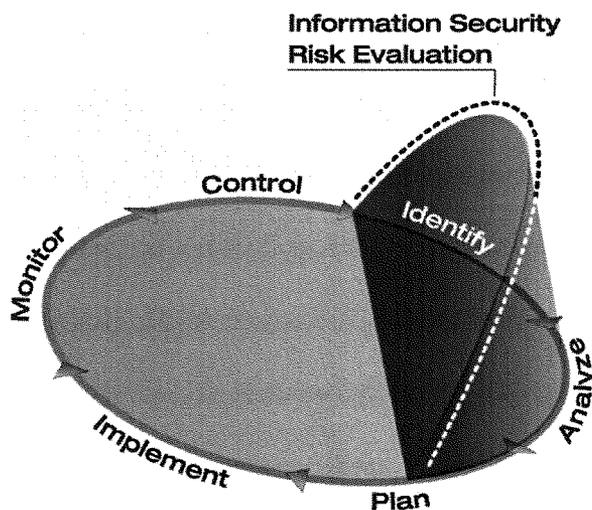


Figure 1: Role of the OCTAVE Methodology in Security Risk Management

(Alberts & Dorofee, 2002)

After completion of the OCTAVE Methodology activities, the organization must complete the Plan step and apply the mitigation plans and protection strategy throughout the remaining security risk management steps.

- *Plan* – Develop detailed plans for the projects, resources, and actions required for implementation.
- *Implement* – Execute action plans, mitigation plans, and a protection strategy.
- *Monitor* - Implement vulnerability management and other means for acquiring data about the status of the infrastructure, and evaluate the effectiveness of plans through audits and other measurement options.
- *Control* – Identify changes in the infrastructure and risk areas that require further analysis. Adjust plans based on those identified changes.

The first version of the OCTAVE Methodology was released for public purchase in September 2001 (<http://www.cert.org/octave>). It was applied first in medical facilities to address the risk assessment required by HIPAA security and privacy regulations (Alberts & Dorofee, 2002). Since September 2001, over 1,000 organizations have used the methodology, including financial institutions, universities, manufacturing companies, and government agencies throughout the world.

### *OCTAVE and Other Security Risk Methodologies*

The Facilitated Risk Analysis Process (FRAP) is considered the most widely used security risk methodology (Peltier, 2003). The FRAP uses an analysis approach similar to the OCTAVE Methodology but does not provide steps for organizational information-gathering activities. Moreover, applying this methodology requires the purchase of

specialized materials and the use of a trained and licensed FRAP facilitator (Peltier, 2001).

Vulnerability analysis was proposed by Parker (1998) to address security risk within the technology infrastructure of the organization. This approach does not fit within organizations with few controls in place, since the evaluation critiques how well existing controls are applied (Peltier, 2001). Also, vulnerability analysis only addresses the technology components of the infrastructure, thereby omitting the organizational security issues (Alberts & Dorofee, 2002).

The Computer Security Institute (CSI) provides an Information Protection Assessment Kit (IPAK) that consists of a questionnaire developed by industry security experts. The IPAK is self-administered and can be purchased through the CSI, but it cannot be tailored (Peltier, 2001).

The use of security risk management is widely recommended by the audit community, and audit methodologies have been expanded to include appropriate practices for IT management (Lanz, 2002). The Information Systems Audit and Control Association (ISACA) sponsors a framework called Control Objects for Information Technology (COBIT) that includes security risk management as an element in the audit review. The American Institute of Certified Public Accountants (AICPA) also developed an information assurance methodology called SysTrust that includes information security risk analysis (Lanz).

## Research Literature Specific to the Topic

K-12 schools and school districts have expanded the use of technology in data gathering and reporting to improve the administrative efficiency of public education (Armstrong, Sibley, & Samara, 2003). This trend is driven by regulatory pressures for increased accountability as established in the NCLB Act and a steady decline of funding available for administration in K-12 schools and school districts (Armstrong et al.). The information security response in K-12 schools and school districts has focused primarily on limiting student and teacher access to Internet content and communication tools such as e-mail (Armstrong et al.). A survey of 811 school districts funded by the National School Boards Foundation (NSBF) cited 91% implementation of content filtering by participant districts (NSBF). The initiative for Safeguarding the Wired Schoolhouse funded through the CoSN provided a list of issues that K-12 schools and school districts should consider when selecting a filtering option (CoSN, 2002). Chapin (1999) identified the need for acceptable use policies (AUPs) along with appropriate physical and technical monitoring to effectively implement content management in K-12 schools and school districts. However, only 19% of the respondents in the NSBF survey reported implementing an AUP. Auditing AUP adherence was addressed by only 2% of the surveyed school administrators, and only 2% reported the establishment of a security position for monitoring Internet and infrastructure activity (NSBF, 2002a).

Higher education has been a focus of national security concern for several years (EDUCAUSE, 2002). Stoll (2000) documented one of the initial discoveries of computer hacking in his analysis of the infrastructure of a higher education institution to determine

the cause for accounting discrepancies in computer usage. Those discrepancies resulted from unexpected levels of activity on dormant computer accounts. By establishing additional dormant accounts seeded with access to fictitious research data and monitoring the network activity on these new accounts, Stoll determined that passwords were systematically guessed to gain access to the system. Once an account was compromised, the account privilege level was elevated providing access to system functions, and operating system capabilities were modified to establish administrative access that provided full computer control to the intruder (Stoll). His research led to institutional changes in account management and acceptable password requirements to reduce opportunities for unauthorized access (Stoll).

University of Delaware administrators Mackenzie and Goldman (2000) described infrastructure-based security problems at this institution that included harassment, illegal hacking, copyright violations, and illegal commercial activity. These problems were subsequently addressed through strengthened security policies and procedures, user education, and increased enforcement mechanisms to identify and punish violators (Mackenzie & Goldman).

At the University of Buffalo, Lesniak (2002), the Director of Academic Services, listed seven key strategies that are applied by this higher education institution:

1. Educating staff, faculty, and students to recognize unsafe practices and understand security threats;
2. Deploying technology tools to protect the infrastructure such as anti-virus software, intrusion detection tools, and firewalls;

3. Monitoring Internet security organizations such as SANS and CERT/CC to identify good practices and new security problems;
4. Prompting the application of vendor-supplied patches on critical systems;
5. Removing unneeded services that are available by default on installed components;
6. Activating and monitoring system logs to identify patterns of abuse; and
7. Creating a response team of key individuals responsible for identifying and repairing security incidents.

Because the infrastructures of K-12 schools and school districts are similar to those of higher educational technology environments (as identified by Updegrave and Long [2001]), each K-12 school and school district should consider applying these same strategies.

The report issued by the President's Critical Infrastructure Protection Board (CIPB) titled *National Strategy to Secure Cyberspace* (CIPB, 2003) provided national visibility to the issues of Internet security. The strategy was issued to "engage and empower Americans to secure the portions of cyberspace that they own, operate, control, or with which they interact" (CIPB, p. 8). A comprehensive national program to "empower all Americans – businesses, the general workforce, and the general population – to secure their own parts of cyberspace" (CIPB, p.13) was identified as a key initiative. Higher education was specifically identified as a component of the critical national infrastructure (<http://www.picb.org>). A strategy focused on the needs of higher education to approach security management within an educational environment was released by EDUCAUSE (2002), an organization for university and college administrators.

Approximately 100 universities and colleges responded to an online survey (<http://www.educause.edu/security/security-survey.html>) that provided input to the EDUCAUSE publication titled *Higher Education Contribution to National Strategy to Secure Cyberspace*.

The Exploring the Future of Learning (EFL) Spring 2003 Forum recommended that “a national K-12 Network Security Initiative be created to provide school leaders with vital information on education security networks, data collection, and acceptable policies in order to ensure privacy and the security of data within their systems” (Armstrong et al., 2003, p. 20). Because of the technological similarities among K-12 schools and institutions of higher education, the EDUCAUSE strategy can ensure that the K-12 Network Security Initiative considers shared critical issues (Updegrave & Long, 2001).

K-12 schools and school districts have not considered the unintended consequences that can arise from inappropriate access to the growing repositories of detailed student records that are accessible using Internet connectivity (Armstrong et al., 2003). According to school administrators participating in a focus group at the EFL Spring 2003 Education Forum, K-12 schools and school districts are amassing detailed student information beyond the needs of current regulatory requirements such as the NCLB Act in anticipation of future needs. However, accountability for controlling access to that information is unclear (Armstrong et al.). Also, school administrators are not considering the need for limitations on the length of time information is maintained in Web-accessible repositories. As a consequence, access to personal information may be available through K-12 school and school district sources permanently (Armstrong et al.).

Each K-12 school and school district must define the appropriate role for technology within its educational curriculum to make effective and appropriate use of technology (Holmes, 1999). The security threats and impacts vary based on the use of technology within each K-12 school and school district, but the need to address relevant risks is common to every entity with Internet connectivity (Peltier, 2001). Security risks are those that represent a potential loss of confidentiality, integrity, or availability to information assets within an infrastructure (Parker, 1998). Identifying security risks that should be considered by K-12 schools and school districts requires the identification of events and related consequences that could result in a non-negligible impact to the entity if the event occurred (Alberts & Dorofee, 2002). Alberts & Dorofee structure a security risk into three components: (1) a security event, (2) a consequence, and (3) a degree of uncertainty. A security event is initiated by a human or natural event that exploits organizational or technological vulnerabilities to invoke a consequence. To reduce the potential impact on the entity, security practices that reduce the likelihood of a security event are applied (Alberts & Dorofee). Each security risk must be linked to one or more security practices that an entity can apply to mitigate the potential impact if the security event occurs.

In a detailed evaluation of references included in this literature review, this investigator applied the structure described by Alberts & Dorofee (2002) to identify security risks relevant to K-12 schools and school districts (see Appendices A and B). For each security risk, the components of event and consequence were identified based on information in the reference source. In addition, associated security practices that would reduce the potential impact of the risk were identified based on the mapping of

information from each literature source to the OCTAVE Catalog of Practices (Alberts & Dorofee). The degree of uncertainty, the third security risk component, is defined within the context of an individual K-12 school or school district and is not meaningful in a general context (Alberts & Dorofee).

Texts and journal articles identified in the bibliography for this dissertation were reviewed to identify K-12 security events. In addition, this investigator monitored the following electronic sources that collect and broadcast security and K-12 domain news and reviewed available archive copies for the period beginning January 2002 to identify specific source documents for K-12 security events to augment literature sources:

- Top Ten Tech Issues provided weekly by *AIG Online* from American International Group, Inc. (<http://home.aionline.com>),
- ComputerWorld Daily Update provided daily by *ComputerWorld* (<http://www.computerworld.com>),
- *SANS News Bites* published weekly by The SANS Institute (<http://www.sans.org/newsletters>),
- TechLearning News published bimonthly by the CoSN and *Technology & Learning Magazine* (<http://www.techLearning.com>),
- *Educational Technology News* published biannually by the North Central Regional Educational Laboratory (NCREL) (<http://www.ncrel.org/tech/etnews>), and
- *Daily Open Source Infrastructure Report* published daily by the U.S. Department of Homeland Security Infrastructure Analysis Infrastructure Protection (DHS/IAIP) (<http://www.nipc.gov/dailyreports/dailyindex.htm>).

To identify the security risks unique to K-12 schools, the security practices assembled by this investigator were compared to a representative set of security practices, specifically, the OCTAVE Catalog of Practices, to identify those not widely used (Alberts et al., 2001). The representative set of security practices were developed from CERT/CC experience and widely accepted standard security practices provided from organizations such as the ISO and NIST. That catalog is referred to as the OCTAVE Catalog of Practices because it is used within methodologies that follow the OCTAVE Approach (Alberts & Dorofee, 2001a).

Security risks and linked security practices identified by this investigator that are not included in the OCTAVE Catalog of Practices are assembled in the table in Appendix A. The security practices that are a part of the current OCTAVE Catalog of Practices and associated K-12 security risks are assembled in Appendix B. The large number of security issues identified as unique to K-12 schools and school districts (see Appendix A) provides a strong indication of the need for a security risk methodology with extensive tailoring capabilities in addressing K-12 school and school district security management (Alberts & Dorofee, 2002).

Identifying evaluation criteria appropriate to the K-12 school and school district is an important part of security risk management. Security threats must have a defined impact based on criteria appropriate to the organization before the threats can be considered risks to the organization (Peltier, 2001). The OCTAVE Methodology uses a set of impact categories derived from research in U.S. Department of Defense medical organizations. These categories include reputation, life and health of customers, productivity, regulatory fines and legal penalties, and financial loss (Alberts & Dorofee,

2002). Regulatory fines and legal penalties, as well as reputation, are potential areas of impact important to K-12 schools and school districts (LeBaron & Collier, 2001). Other impact categories that establish evaluation criteria appropriate to the K-12 school environment are suggested by Norris, Soloway, and Sullivan (2002) in their review of technology use in education:

- Insufficient access to technology for students and teachers – No specific target levels are identified, but a one-to-one relationship is projected as needed.
- Teacher preparation and technology support – Training in technology use, techniques for incorporating technology into classroom use, and technical support of Internet connectivity.
- Student achievement results – Changes in student achievement that are traced to use of Internet connectivity will impact technology access.
- Financial support for school and school district administration – Limitations to provisions for funding teacher and student training, and limitations in technical support to maintain an appropriate working level of the technology could severely impact Internet connectivity.
- Community reputation – The reputations of K-12 schools and school districts in the community could be impacted by the inappropriate use of technology.

The Exploring the Future of Learning (EFL) Spring 2003 Education Forum identified student information privacy and educational effectiveness as defined by the NCLB Act as key areas of impact on each school (Armstrong et al., 2003). Failure to maintain student information privacy could enable high impacts such as identity loss and inappropriate physical access to a child. Failure to meet the effective educational

standards could lead to increased regulatory monitoring, remedial actions, and possible school closings if a sufficient number of students transfer to other schools (Armstrong et al.).

### **Summary of What Is Known and Unknown About the Topic**

Anthony and Cohn (2002) documented the need for parental control of Internet interactions for a child to assure protection of that child's privacy. Armstrong and Casement (2000) identified limitations of technology in meeting educational requirements for every child. Caregivers and parents are on both sides of this issue. Some are exerting efforts toward greater control in the protection of their children by prohibiting Internet access in schools and libraries (Bradsher, 2000). Others are pressing to expand the use of technology within the classroom as a mandate for effective education (Armstrong & Casement). Regulations related to Internet access in K-12 schools and school districts such as the COPA and CDA have been implemented and removed by the courts (Hunter, 2000). The usage requirements for E-rate funding defined in the CIPA mandated the implementation of content-blocking capabilities in K-12 schools and school districts by July 2002 (Heins, 2001). However, these requirements, like earlier regulations, have been challenged in the courts and may be removed (Pruitt, 2003).

The reactions of 811 school administrators to technology security issues as summarized by the National School Boards Foundation (NSBF) show the focus for security protection on content-blocking with less consideration of other security concerns such as anti-virus protection, acceptable use policies (AUPs), and auditing (NSBF,

2002b). To meet reporting requirements for the No Child Left Behind (NCLB) Act of 2001, K-12 schools and school districts continue to expand extensive data repositories with sensitive information for use by local, state, and federal officials via the Web (ED, 2001), thereby expanding opportunities for the inappropriate use of that information.

Information gathered by the CERT/CC shows that the number of vulnerability incidents doubled each year between 1998 and 2003 (Pethia, 2003). Analysis of these incidents indicates that increased availability of enhanced attack tools contributes to the capability of individuals to initiate attacks with broader impact (Carpenter, 2001). Available tools are capable of compromising large volumes of Internet-connected sites just minutes after a vulnerability is exposed (Carpenter). These tools are disseminated to all interested individuals through Internet communication facilities such as bulletin boards, chat rooms and listservs (Pethia). Responding to each vulnerability incident as it is identified is no longer a reasonable approach to security management (Pethia).

A compromise can lead to disclosure and modification, as well as the permanent loss of information or temporary loss of access (Parker, 1998). According to Richardson (2003), survey results by the San Francisco FBI Computer Intrusion Squad (CIS) indicated that 530 computer security practitioners from U.S. corporations, government agencies, financial and medical institutions, and universities reported heavy financial losses involving Web-initiated intrusions. Currently in its eighth year, the FBI survey documents problems that persist each year with growing frequency and expanded impact as organizational reliance on technology increases (Richardson).

The Technology Standards for School Administrators (TSSA) and International Society for Technology in Education (ISTE) promote the expanded use of technology

within the K-12 school environment for administration, teaching, and learning (TSSA, 2001). Funding sources such as the U.S. Department of Education (ED) support the expansion of technology in K-12 schools and school districts. However, security considerations are not included as part of the evaluation results (ED, 2000a). Regardless of the reason, incorporating technology into the K-12 classroom introduces security issues that must be addressed once connectivity to outside networks is implemented (Parker, 1998). Cases of children in the sixth grade using poor security practices to illegally adjust grades have been reported (Shah, 2003). Moreover, high-school students use tools readily available on the Internet to break into school databases and change information (Akizuki, 2003).

In K-12 schools and school districts, minimum standards of best practice are not yet established (Armstrong et al., 2003). Limitations of time, money, and technical expertise have conspired to promote less than optimal solutions (Cuban, 2001). Technology use in the classroom is inconsistent, resulting in a wide variance of security risk among K-12 schools and school districts. Students and parents continue to demand a greater use of technology in education, increasing the potential for security risk (ISTE, 2002). Reliance on volunteer assistance and student technical expertise increases the need for security risk management (Armstrong et al.).

Security risk from Internet-connected sources increases annually (Schneier, 2000). K-12 schools and school districts can benefit from applying general security practices (see Appendix B) but require the ability to tailor a selected security risk methodology to meet the needs related to domain-specific issues (see Appendix A). Financial and technical resources for technology support available in the K-12 schools

and school districts are limited with strong indications that greater limitations will be forthcoming (NSBF, 2002a). Extensive help from volunteers and student assistants is needed to meet current minimal support levels (Cuban, 2001).

Many types of security risk methodologies are available for addressing information technology risk, but many widely used options involve a purchase fee and special training. In addition, many require the inclusion of areas such as auditing, which extend beyond the scope of this research effort (Lanz, 2002). To meet the domain-specific requirement for K-12 schools and school districts, a methodology with extensive tailoring capabilities is required. The OCTAVE Methodology fulfills these requirements (Alberts & Dorofee, 2002).

### **The Contribution this Study Makes to the Field**

When an information security risk methodology that addresses the unique needs of K-12 schools and school districts is applied, improvements in security management are possible. Improvements for K-12 schools and school districts can be similar to those experienced by U.S. health care organizations, financial institutions, government agencies, and manufacturing organizations in which information security risk management is already widely adopted (Alberts & Dorofee, 2002). K-12 technology planners can use the tailored security risk management methodology to articulate requirements, identify accompanying security risks, and define good security practices to address unacceptable levels of security risk (Alberts & Dorofee). As a result, technology planners for K-12 schools and school districts can consider security risk management as

part of the technology-related needs of their students, teachers, student's parents, and the local community.

This researcher identified the information security requirements for K-12 schools and school districts through a broad literature review. These requirements were applied to the OCTAVE Methodology using in-place tailoring capabilities. The tailored methodology was used at a selected K-12 school district and reviewed by K-12 experts, confirming the validity of the identified requirements. A framework for identifying and prioritizing information security risk focuses attention and resources on security issues with the greatest impact (Alberts & Dorofee, 2002). A self-directed information security assessment for use by K-12 schools and school districts is of great interest to the Consortium for School Networking (CoSN) as identified by Keith Krueger, CoSN Executive Director (personal communication, July 31, 2003). With a methodology tailored to meet their needs, K-12 school administrators can proactively construct and evaluate the ability of their networking solutions to facilitate safe and secure access to Internet-accessible resources.

A correlation exists between the security threats identified within higher education such as those reported by administrators at the University of Delaware (Mackenzie & Goldman, 2000) and those expected in K-12 schools and school districts. That correlation indicates that a successful security risk methodology tailored to the unique needs of K-12 schools and school districts would also be of value to technology planners in higher education. Higher education is one of the critical sectors for national security as identified in the CIPB (2003) *National Strategy to Secure Cyberspace* report. Members of the EDUCAUSE/Internet2 Security Task Force plan to review the K-12 Risk

Methodology as part of the development process for a risk methodology tailored for higher education and based on the OCTAVE Approach (Rodney Peterson, Security Task Force Project Coordinator, personal communication, October 29, 2003).

K-12 schools and school districts have no regulatory mandate for information security and have not addressed security risks (Updegrove & Long, 2001).

Documentation of the steps taken and issues encountered while identifying security requirements and applying a security risk methodology tailored to K-12 schools and school districts provides a template for inserting a security risk management process into organizational sectors that exhibit limited recognition of security risk (Armstrong et al., 2003).

## Chapter 3

### Methodology

#### **Research Method Employed**

K-12 schools and school districts increasingly support expanded Internet connectivity. However, survey results issued by the National School Boards Foundation (NSBF, 2002a) indicate a lack of recognition by school administrations of the need for protecting users and devices connected to the Internet through the K-12 infrastructure. Moreover, an understanding of the importance of monitoring K-12 Internet connectivity to ensure that its use is limited to legitimate functions is also lacking (NSBF). The Internet is by design an environment of trust (Schneier, 2000). Security options were developed and applied as participation expanded exponentially and the validity of trust provided in the original design proved inappropriate (CIPB, 2003).

Medical organizations must perform periodic technology risk assessments under the Health Insurance Portability Accountability Act (HIPAA) provisions (DHHS, 2003). Provisions of the Gramm-Leach-Bliley Act (GLBA) of 1999 require financial institutions to perform a security risk assessment (Lanz, 2002). The Government Information Security Reform Act (GISRA) requires every U.S. government agency to perform a security risk assessment to assure the appropriate levels of security protection needed for continued technology funding from federal sources (Swanson, 1998). Based on the

number of regulatory mandates across a wide range of organizational domains, K-12 schools and school districts should consider the importance of applying a security risk assessment (Armstrong et al., 2003).

The lack of clear standards for good security and confusion over appropriate security assessment mechanisms motivate organizations to apply risk management in the area of information security (Peltier, 2001). Lanz (2002) reported options for security risk management that were considered by the American Bankers Association (ABA). The framework sponsored by the Information Systems Audit and Control Association (ISACA) and called Control Objects for Information Technology (COBIT) was included. The American Institute of Certified Public Accountants (AICPA) information assurance service called SysTrust was included. Additionally, the OCTAVE Methodology and the NIST Self-Assessment 800-26 used by federal agencies to validate federal regulatory compliance were included for consideration.

Lanz (2002) noted that COBIT and SysTrust are broad audit assessments covering much more than security. According to Lanz, the OCTAVE Methodology is a comprehensive self-directed approach for large organizations using risk considerations to first determine which information assets need protection, and then define how protection should be applied based on security practices assembled from academia and industry. Lanz reported that the NIST Self-Assessment 800-26 is focused primarily on U.S. government security regulations.

In addition to the options identified by the ABA, Peltier (2001) identified the Facilitated Risk Analysis Process (FRAP) as the most widely used security risk assessment methodology in business and finance. The OCTAVE Methodology and the

NIST Self-Assessment 800-26 are both self-directed and available via the Web at no cost. The OCTAVE Methodology can be tailored to fit the unique context of an organization (Alberts & Dorofee, 2001), but the NIST self-assessment requires strict adherence to the specifications established within the methodology (Swanson, 2001). The FRAP is applied by security experts who are trained and licensed to deliver the methodology (Peltier). An Information Protection Assessment Kit (IPAK) consisting of a series of questions developed by security experts can be purchased from the CSI, but no tailoring options are available for it (Peltier).

This researcher used the OCTAVE Methodology for this investigation in applying security risk management for Internet connectivity in K-12 schools and school districts. The methodology accommodated financial limitations for technology usage in K-12 schools and school districts (CoSN, 2002). The methodology does not attempt to impose those regulatory compliance requirements appropriate for banks or hospitals. K-12 schools and school districts lack specific security regulations beyond content filtering (NSBF, 2002a). The methodology supports the unique context of the educational environment, which requires a blending of academic and business needs with limited technical support expertise (Cuban, 2001). Also, the methodology does not enforce any general auditing requirements that exceed the proposed focus of this research effort (Lanz, 2001).

The OCTAVE Methodology takes into account the unique characteristics of each individual K-12 school and school district. In addition, this methodology provides a comparison of current security procedures to the general best practices assembled from the security standards of the BSI, NIST security recommendations, and the CERT/CC

vulnerability analysis (Alberts et al., 2001). Moreover, the OCTAVE Methodology provides a systematic process for guiding a K-12 school or school district in the identification of its unique security risks and the development of a plan for addressing those risks (Alberts & Dorofee, 2002). The OCTAVE Methodology has been implemented by over 1,000 medical, government, university, financial, and manufacturing operations throughout the world (<http://www.cert.org/octave>). The U.S. Department of Defense medical community has selected the OCTAVE Methodology to meet its mandated security risk assessment requirement for compliance with Health Insurance Portability Accountability Act (HIPAA) regulations (DHHS, 2003). The OCTAVE Methodology is publicly available as part of the SEI program to improve the overall state of security risk management in networked environments (Alberts & Dorofee).

For this study, this investigator tailored the OCTAVE Methodology using options provided within the methodology (Alberts & Dorofee, 2002). Although the methodology was constructed for large organizations, tailoring options were available to streamline the steps for any size entity (Alberts & Dorofee). The tailored methodology was validated as being appropriately based on the OCTAVE Approach through the use of the OCTAVE Criteria. The OCTAVE Criteria consist of principles, attributes, and outputs that define the required elements of risk management for an effective security risk management evaluation using the OCTAVE Approach (Alberts & Dorofee, 2001a). Validation of the tailored methodology using the OCTAVE Criteria confirmed that tailoring adjustments did not impact the value of the security risk assessment (Alberts & Dorofee, 2002).

The tailored methodology is referenced throughout this dissertation as the K-12 Risk Methodology. A tailored methodology that continues to carry the OCTAVE name requires licensing from Carnegie Mellon. Based on previously identified financial resource limitations for technology in K-12 schools and school districts, the added licensing cost of using the OCTAVE name was deemed a deterrent by Steve Miller, CoSN Executive Board member (personal communication, February 24, 2003). As a consequence, the OCTAVE Methodology is referenced as the basis for the K-12 Risk Methodology, but the OCTAVE name is removed from all documents within the tailored version (<http://www.cert.org/octave/licensing.html>).

The OCTAVE Methodology addresses the overall planning aspects for Internet security within the K-12 school and school district, and not the details of applying security technology within the school environment (Alberts & Dorofee, 2002). The OCTAVE Methodology establishes a general process for the initial development of information security plans to protect information assets within the organization. Approaches for including evaluation results within the continuous planning cycles of an organization, as well as acquisition strategies for new technology, are suggested but not specifically provisioned within the OCTAVE Methodology (Alberts & Dorofee).

#### *OCTAVE Methodology Description*

The OCTAVE Methodology is applied through a series of structured workshops performed by an analysis team composed of carefully selected individuals who represent the range of technology interests and responsibilities across the organization (Alberts & Dorofee, 2001c). The members of the analysis team must assemble their individual knowledge into a shared perspective to define both the current technology security

environment and the needs of the organization that technology must support. This effort can take from three days to two months depending on the level of effort applied by analysis team participants (Alberts & Dorofee, 2002). OCTAVE Methodology workshops are grouped into three phases: (1) Organizational View, (2) Technological View (which is optional), and (3) Security Strategy and Planning.

### Phase 1: Organizational View

In the first phase, the analysis team establishes the organizational view through the identification of information assets (systems, software, applications, and people) that are important to the organization. For each asset, security requirements are identified. Moreover, the organizational perspective of how the information is protected and/or threatened by the existing environment is ascertained. From the first phase, the analysis team selects the most critical information assets, generally three to five, to carry forward to the remainder of the process. Assets that represent large adverse effects when their security requirements are violated are considered critical assets (Alberts & Dorofee, 2001c). For each selected critical asset, threats to confidentiality, integrity, and availability are identified and assembled into threat profiles (Alberts & Dorofee, 2001b).

The activities in Phase 1 support the assembly of an organizational view of assets, threats, vulnerabilities, and current security practices. Assets are identified through a series of facilitated workshops with participants from several organizational layers, including senior management, operational management, administrative staff, and technical staff. Current security practices and organizational vulnerabilities that could adversely impact the assets are also identified. Each workshop group selects the three to five most important assets from their list of important assets and identifies the security

requirements that should be in place to protect them. The analysis team summarizes the information collected from all the workshops for use in subsequent methodology activities. From that summary, the team selects three to five critical assets and refines the security requirements to carry forward through the remainder of the evaluation as a representative sample of all the organizational assets (Alberts & Dorofee, 2001a). For critical assets, threat profiles are constructed using generic threat profiles based on the summarized organizational vulnerabilities identified in the workshops and gaps identified in the current security practices (Alberts & Dorofee, 2001b). The final outputs of Phase 1 are the following:

- Organizational assets, organizational security concerns, and security requirements summarized from a series of data collection workshops;
- Critical assets selected by the analysis team and related security requirements them;
- Threats to critical assets identified using generic threat profiles; and
- Current security practices.

### Phase 2: Technological View

In the second phase, which is optional, the analysis team plans and executes a targeted vulnerability assessment to identify weaknesses in the technology infrastructure that confirm and augment the threat profiles for the critical assets developed in the Phase 1. Components of the infrastructure that are linked to each critical asset and relevant to processing, storing, or transmitting data are selected for assessment. Firewalls, routers, and switches, as well as external service providers and links from other devices that provide access paths to critical assets, are also selected for assessment (Alberts &

Dorofee, 2002). Phase 2 is performed only when the organization can readily hire individuals experienced in vulnerability management to perform the assessment (Alberts & Dorofee, 2001c).

The vulnerability information is used to identify major weaknesses in the infrastructure that need immediate attention and to define ways the technology allows for asset compromise (Allen, 2001). In addition, vulnerabilities may represent additional threats to critical assets that augment the threats assembled during Phase 1 (Alberts & Dorofee, 2001a). The outputs of Phase 2 include the following:

- Infrastructure components important to each critical asset, and
- Summarized technological vulnerabilities from the targeted assessment of selected components.

### Phase 3: Security Strategy and Planning

In the third phase, the analysis team defines the organizational impact of each threat identified in the prior phases. The combined threat and corresponding impact represent a risk to the organization that must be considered for acceptance or mitigation. Evaluation criteria that define the level of concern an impact represents to the organization are assembled. The evaluation criteria allow the analysis team to quantify risks (high, medium, or low) so that resources for protection can be applied to risks that represent the greatest organizational impact. Risk mitigation plans for each critical asset are developed to address high-impact risks by analyzing the gaps between the organization's current security practices and best practices described in the OCTAVE Catalog of Practices. The analysis team develops an organizational protection strategy by reviewing the risk mitigation plans for the critical assets to identify commonalities that

should be applied broadly across the organization. Results are assembled into a series of reports that identify near-term actions, mitigation plans focused on specific information assets, and an organizational protection strategy that identifies the framework for establishing the appropriate protection for current and future assets (Alberts & Dorofee, 2002).

Evaluation criteria to prioritize financial impacts and threats to health and safety, productivity, fines and legal penalties, and reputation are suggested by the methodology as a reasonable baseline for impact analysis (Alberts & Dorofee, 2002). Each critical asset risk is analyzed using the evaluation criteria and valued to provide a scale for prioritization. Security practices that need improvement are compared to the highest priority risks to identify the practices most needed by the organization. The analysis team identifies immediate, near-term, and long-range activities for applying security practices that address the highest risks to critical information assets (Alberts & Dorofee, 2001a). The analysis team presents the proposed plan to the organizational decision makers to obtain approval from appropriate groups within the organization to carry the plan forward to implementation. The outputs of Phase 3 are the following:

- Risk measures, also called evaluation criteria;
- Risks to critical assets;
- Action items or plans for immediate activities;
- Mitigation plans or plans for near-term activities related directly to critical assets;
- and
- Protection strategies or plans for long-range activities across the organization.

### *OCTAVE Criteria Principles*

The OCTAVE Methodology is based on the OCTAVE Criteria principles, attributes, and outputs that define the required elements of risk management for an effective security risk management evaluation using the OCTAVE Approach (Alberts & Dorofee, 2001a). Principles are defined as fundamental concepts of risk management that must drive the nature of the evaluation. Attributes are characteristics of a successful evaluation for risk management. Outputs define the results that must be achieved to accomplish a successful evaluation. The tailored methodology must incorporate the OCTAVE Criteria to validate its application of the OCTAVE Approach for security risk management (Alberts & Dorofee).

The principles in OCTAVE Criteria define key concepts that describe the nature of the evaluation (Alberts & Dorofee, 2002). These principles are built from the SEI research experience in risk management, organizational management, and information security risk management and each is described in the remainder of this section (Alberts et al., 2000):

- From SEI experience in information security risk management, the principles of self-direction, adaptable measures, defined process, and foundation for a continuous process are drawn (Alberts & Dorofee).
- From the field of risk management, the principles of forward-looking view, focus on the critical few, and integrated management are included (Alberts & Dorofee).
- From organizational management, the principles of open communication, global perspective, and teamwork are drawn (Alberts & Dorofee).

## Principles from Security Risk Management

The self-direction principle allows people in the organization to manage and direct the evaluation process. This principle is based on the assumption that personnel in the organization understand how to manage organizational risk, but must be guided in identifying and managing security risk (Alberts & Dorofee, 2001a).

The adaptable measures principle results in the application of flexible measurements that are adapted to work within the unique context of the organizational environment. Available measurements include known security threats and known technological weaknesses that are identified by authoritative sources such as the CERT/CC and the Mitre Corporation (Alberts & Dorofee, 2001a).

The defined process principle requires the use of standardized evaluation procedures within which the analysis team is required to assign each activity or action to a responsible individual or group (Alberts & Dorofee, 2001a). The procedures used by the analysis team include: defining all evaluation activities, assigning responsibilities for each evaluation activity, specifying evaluation mechanisms, and creating a common format for documenting evaluation results. Defined evaluation procedures are structured from template worksheets including detailed instructions that make up a structured and consistent framework for the identification and analysis of security risk. In addition, documentation within the methodology of the processes used to identify risks, impacts, and plans in addressing critical risks contributes to defined evaluation procedures (Alberts & Dorofee).

The foundation for a continuous process principle establishes security management as ongoing. Each evaluation provides a framework for the identification,

analysis, and planning of security requirements for the organization. This framework forms the basis for implementing, monitoring, and controlling information security to complete the cycle of continuous security management (Alberts & Dorofee, 2001a).

### Principles from Risk Management

The forward-looking view principle enables participants to look beyond the existing environment and establish a protection strategy that will allow for continuous change. Change can occur in the composition of an organization's information assets and the technology infrastructure that supports the assets. Change can also be triggered by threat events that are initiated either internally or externally and that put the infrastructure and assets of the organization at risk (Alberts & Dorofee, 2001a).

The focus on the critical few principle provides a mechanism for addressing security risk within the limitations of organizational resources. The efficient use of these resources focuses organizational attention on the highest priority risks. The methodology is structured to provide an effective and efficient means for limiting the volume of data under consideration at each activity (Alberts & Dorofee, 2001a).

The integrated management principle points to the need to have security policies and strategies consistent with overall organizational ones. Trade-off choices made in organizational policy setting at the highest levels of the organization must be reflected consistently in the choices applied to security policy (Alberts & Dorofee, 2002).

### Principles from Organizational Management

The open communication principle emphasizes the need for broad participation across many areas of the organization. A collaborative effort is required to assemble

information and develop decisions that are shared among participants assembled across the organization (Alberts & Dorofee, 2002).

The global perspective principle requires that consensus be reached in addressing security issues since it would be ineffective for one part of the organization to act under one set of policies and procedures while other parts of the organization use a different set. Security requires consistency at all levels across the organization to appropriately address threats to the organization (Alberts & Dorofee, 2002).

The teamwork principle emphasizes the challenges involved in dealing with an issue as complex as information security. No one individual or group of individuals can have all the knowledge and requisite response information. Information must be pooled from the broad range of participants within the organization and possibly include experts outside of the organization to assemble data and develop the appropriate plans that address the security needs of the organization (Alberts & Dorofee, 2002).

### *OCTAVE Criteria Attributes*

Attributes define the structure of each process within the methodology and establish essential elements that must be present for an appropriate application of the OCTAVE Approach (Alberts & Dorofee, 2001a). Within the OCTAVE Criteria, attributes establish the characteristics of the principles. The following attributes are included in the OCTAVE Criteria: analysis team, augmentation of analysis team skills, catalog of practices, generic threat profile, catalog of vulnerabilities, defined evaluation activities, documented evaluation results, evaluation scope, next steps, focus on risk, focused activities, organizational and technological issues, organizational and information technology participation, senior management participation, and collaborative

approach. Along with principles, attributes must be maintained when any tailoring is applied to assure consistency with the OCTAVE Criteria (Alberts & Dorofee). A summary list of principle and attribute links is provided in Appendix C. Some principles map to multiple attributes, and some attributes link to multiple principles (Alberts & Dorofee). A description of each attribute, grouped by the principle to which it applies, is provided below.

### Attributes for Self-Direction

An analysis team composed of personnel from within the organization is assembled to lead the evaluation activities. Personnel who use technology within the organization, as well as technology specialists who implement and support the organization's infrastructure, must work together to forge a unified view of the security risk from an organizational perspective. The organization's leadership must take ownership of identified information risks and agree to the steps developed by the analysis team to address the risks, thereby ensuring that appropriate measures will be taken to implement plans built using the OCTAVE Approach (Alberts & Dorofee, 2001a).

Augmentation of analysis team skills extends the ability of the organization to address the complexities of security management and the challenge of assembling a sufficiently strong team to cover all needed aspects. This attribute provides a mechanism for adding skills without transferring organizational responsibility. Through the selective expansion of the team to address specific areas where analysis team skills are limited, the OCTAVE Approach provides a mechanism for addressing skill and knowledge variations without jeopardizing ownership and responsibility for the results (Alberts & Dorofee, 2001a).

### Attributes for Adaptable Measures

Use of a catalog of practices ensures that the organization will consider the range of strategic and operational security practices important for good security risk management. The OCTAVE Catalog of Practices is assembled from experience at the CERT/CC in responding to reported Internet vulnerabilities, results from the SEI's experience in performing security evaluations, and security practices from recognized international standards organizations such as the British Standards Institution (BSI). The BSI published a code of practices in 1995 that was adopted in 2000 by the International Standards Organization (ISO) as ISO 17799 (Brykczynski & Small, 2003). The OCTAVE Catalog of Practices incorporates the practices from the BSI publication BS 7799: Part 1: 1995 (BSI, 1995). That body of knowledge provides a basis of security best practices against which an organization can measure its own internal efforts and identify opportunities for improvement (Alberts et al., 2001).

With the use of a generic threat profile, the organization considers a range of threats that are formalized into structured profiles (Alberts & Dorofee, 2001b). A threat represents a potential combination of a security event source identified as an threat actor performing a deliberate or accidental action that results in an undesirable outcome. The outcomes are security compromises to information assets that result in disclosure, modification, loss/destruction, or interruption, thus causing undesirable consequences for the organization (Alberts & Dorofee, 2001a). The OCTAVE Methodology incorporates four structured threat profiles representing threats from four actor sources: (1) human actors using network access, (2) human actors using physical access, (3) system problems

such as hardware and software defects, and (4) other problems such as floods and power outages (Alberts & Dorofee, 2001b).

Using a catalog of vulnerabilities assures that infrastructure vulnerabilities are evaluated in terms of standard sources such as the Common Vulnerabilities and Exposures (CVE). The CVE consists of a list of known vulnerabilities developed collaboratively by security professionals and maintained by the Mitre Corporation (<http://cve.mitre.org>). The list also provides characteristics of vulnerabilities so that security experts and assessment tools can detect when a specific vulnerability is present in an infrastructure. A severity rating for each vulnerability (high, medium, or low) based on the ease of its exploit by an unsophisticated attacker is provided in the CVE along with instructions for removing the vulnerability (Alberts & Dorofee, 2001a). It is important to note that the volume of reported vulnerabilities is doubling annually with no expected rate decrease (Pethia, 2003).

#### Attributes for Defined Process

Defined evaluation activities ensure that a well-structured and comprehensive evaluation is performed. Procedures are specified for the series of workshops required to perform the methodology. Detailed instructions, provided for each workshop, include preparation activities, task lists, worksheet templates, examples of anticipated outcomes, and reference catalogs to be used. This level of definition provides a repeatable process that serves as the framework for an ongoing risk management effort. Moreover, the steps in the process and expected outcomes can be evaluated in advance of resource commitment, thus, providing a means of establishing appropriate expectations for decision makers. Tailoring requirements for specific types of organizations can be

identified and incorporated in advance for each required activity (Alberts & Dorofee, 2001a).

With documented evaluation results, the sponsoring entity, or in this case the K-12 school or school district, records the information captured within each activity to produce a body of material that represents the organization's use of the OCTAVE Methodology. That material becomes a permanent record that defines the security risks of the organization and represents a formal attempt to address risks outside of acceptable organizational tolerance levels. The documented results support implementation decisions that are part of security mitigation plans and protection strategies (Alberts & Dorofee, 2001a).

The evaluation scope must be delineated carefully to assure inclusion of critical organizational areas within the assessment. The resource and time limitations established by organizational decision makers must be considered when defining the segments of the organization to be included in the evaluation. Large and complex K-12 schools or school districts can manage the scope by including only a few departments critical to their mission. These departments should represent a good sample of the K-12 school or school district as a whole (Alberts & Dorofee, 2001a).

#### Attributes for Foundation for a Continuous Process

With the next steps, the OCTAVE Methodology is formally recognized as a basis for planning. Effective adoption requires that plans developed within the OCTAVE Methodology provide the basis for subsequent implementation as part of a complete risk management process. Decision makers review the results of the evaluation process and

determine follow-up actions to appropriately manage the security risks identified through the application of the methodology (Alberts & Dorofee, 2001a).

Senior management participation communicates active sponsorship to members of the organization. Implementing plans to manage security risks requires resource commitments from the leadership of the organization. Through active participation in the process, decision makers gain an understanding of the importance of security risk management and ensure that the mission, risk tolerance, and resource limitations of the organization are represented appropriately (Alberts & Dorofee, 2001a). In addition, the attribute catalog of practices, described previously with adaptable principles, applies to the principle foundation for a continuous process.

#### Attribute for Forward-Looking View

A focus on risk requires consideration of the impact of potential threats instead of simply the identification of all possible threats. Scarce resources are allocated to the highest priority risks - those that would result in the greatest potential harm to critical assets of the organization (Alberts & Dorofee, 2001a).

#### Attributes for Focus on the Critical Few

Focused activities facilitate the delineation of security risk issues impacting important information assets. A comprehensive view of all assets, all vulnerabilities, and all security issues is not addressed within the methodology. The analysis process is complex and becomes ineffective if too broad a perspective is attempted (Alberts & Dorofee, 2001a). In addition, the attribute evaluation scope, described with the defined process principle, applies to the focus on the critical few principle.

### Attributes for Integrated Management

Organizational and technological issues must be examined in the security evaluation. Security threats and serious risks can result from inappropriate and ineffective organizational policies and practices. Moreover, serious risks can result when technology vulnerabilities are not effectively addressed in the infrastructure (Alberts & Dorofee, 2001a). Activities within the methodology are structured to incorporate both the organizational and technological views, which are critical to the formulation of an effective protection strategy (Alberts & Dorofee). If an organization relies only on vulnerability assessment tools to evaluate the security risk of the infrastructure, the assessment will address only a small segment of the security risks that should be considered (Alberts et al., 2001). Vulnerability tools identify known weaknesses in the technology, improper configurations of administrative functions such as accounts with null passwords, and information a possible attacker can use to locate infrastructure weaknesses (Parker, 1998). Vulnerability tools do not identify improper systems administration that allows access to the wrong individuals, unknown vulnerabilities that may allow future inappropriate access, or incorrect applications of policies and procedures (Alberts & Dorofee, 2002).

Organizational and information technology participation is required to address the principle of integrated management. A range of perspectives across the organization is necessary to identify the assets, threats, security requirements, and risks that are critical to the organization. Without strong organizational participation in the evaluation's activities, the mission of the organization cannot be represented properly, and without strong technology participation, the infrastructure risks are not identified properly. A

balanced perspective assures the appropriate consideration of both organizational and technological issues (Alberts & Dorofee, 2001a). In addition, senior management participation, described earlier in this report under the heading of Attributes for a Foundation for a Continuous Process, applies to the principle of integrated management.

#### Attribute for Open Communication

A collaborative approach for sharing information and building consensus in decision making is required to ensure that the broad range of perspectives represented by analysis team members is considered in the evaluation. Participants see the value and accept responsibility for implementing resulting plans if they are part of the process that identifies the needs and establishes the plans (Alberts & Dorofee, 2001a).

#### Attributes for Global Perspective

The attributes referenced as organizational and technological issues and organizational and information technology participation, described earlier in this dissertation under the heading of Attributes for Integrated Management, apply to the principle of global perspective. Based on the application of other principles such as open communication, the blending of participants from across the K-12 school or school district should yield a global perspective.

#### Attributes for Teamwork

The attributes described earlier in this dissertation under the heading of Attributes of Self-Direction, namely analysis team and augmenting analysis team skills, apply to the principle of teamwork. The attribute described earlier under the heading of Attributes of Open Communication, namely collaborative approach, applies to the principle of

teamwork as does the organizational and information technology participation attribute described under the heading of Attributes of Integrated Management.

### **Specific Procedures Employed**

A tailored version of the OCTAVE Methodology to support this investigation was designed for use in the K-12 schools and school districts (Alberts & Dorofee, 2002). The unique requirements of the K-12 technology environment identified in the literature search and the security practices unique to K-12 schools and school districts listed in Appendix A were incorporated into the OCTAVE Methodology. The OCTAVE Catalog of Practices and each activity, along with worksheets and step-by-step instructions, were modified as needed to build a methodology uniquely tailored for this domain (Alberts & Dorofee, 2001). Based on a review by Christopher Alberts, an SEI researcher and developer of the OCTAVE Methodology, of the unique needs of K-12 schools and school districts that are relevant to information security (C. Alberts, personal communications, December 13, 2002), the following tailoring options within the OCTAVE Methodology were selected for consideration:

- Expansion of the OCTAVE Catalog of Practices incorporating requirements unique to K-12 schools and school districts.
- Adjustment of the data-gathering process used in the workshops for Phase 1: Organizational View that is currently based on a hierarchical organization structure, allowing for the collection of asset and security requirements from a distributed organizational structure that included administrative staff, teachers, parents, and students. Schools comprise a blend of three sub-organizations that

must be represented within the Organizational View. These sub-organizations include administration to address the business processes of the K-12 school or school district such as payroll and purchasing; teaching to address classroom instruction and information distribution; and learning to address student participation that may extend to parental involvement.

- Augmentation of the guidelines and worksheet templates for defining threats to an asset to provide a means for explicitly identifying authorized and unauthorized individuals or groups of individuals. In the OCTAVE Methodology, individuals who hold organizational positions that enable them to access an asset are called insiders, and individuals or groups that should be denied access to an asset are called outsiders. The designation of insiders and outsiders within a K-12 school or school district is inconsistent and must be qualified for each asset. For example, for classroom assignment folders, students and teachers are insiders and administrative personnel are outsiders. For the payroll system, administrative personnel are insiders and students are outsiders.
- Adjustment of evaluation criteria to categories important to K-12 schools and school districts. Productivity, reputation, and customer confidence, suggested by the OCTAVE Methodology as evaluation criteria, are not as important in K-12 school and school district settings as regulatory compliance, curriculum effectiveness, student performance on standardized tests, and community support (Norris et al., 2002).

- Adjustment of the terminology used in worksheets and instructions developed for medical, manufacturing, financial, and government agencies to incorporate K-12 school and school district terminology.

The following steps, described in greater detail in Chapter 4, were performed by this investigator to build the prototype K-12 Risk Methodology:

- Identified security risks relevant to K-12 schools and school districts and security practices that mitigate the risk from the literature search (see Appendices A and B).
- Expanded the OCTAVE Catalog of Practices to incorporate each security practice unique to K-12 schools and school districts from Appendix A.
- Examined the tailoring options within the OCTAVE Methodology to understand the relationships among steps in the process and determine how changes to one area impacted other parts of the methodology.
- Applied the tailoring options selected for consideration as appropriate to K-12 school and school district requirements. The selection process is described earlier in this section of this document.
- Evaluated the tailored methodology to assure compliance with the OCTAVE Criteria.
- Performed a risk evaluation using the tailored methodology at a selected K-12 school district. This process is further described in the remainder of this section and in Chapter 4.

- Reviewed the methodology with experts from various K-12 schools and school districts to confirm broad applicability. This process is further described at the end of this section and in Chapter 4.

Based on the SEI's experience with inserting the OCTAVE Methodology into multiple domains, this researcher determined that not every unique requirement for this inquiry would be identifiable from the literature review (Alberts & Dorofee, 2002).

Following the approach used in the development of the OCTAVE Methodology for the U.S. Department of Defense medical community, this researcher selected a pilot site for a facilitated use of the K-12 Risk Methodology to identify additional tailoring needed to fit the methodology to needs of the K-12 schools and school districts (Alberts & Dorofee).

Participants at the pilot site were required to learn and apply the tailored methodology for their school and evaluate the results of the methodology, as well as the applicability to their school setting. To be considered for the pilot site, the K-12 school or school district was required to have the full age range of students and actively use technology within the curriculum at most grade levels. To assure on-site availability and eliminate conflicts with vendor contract provisions, technology support personnel were required to work for the school or school district rather than an external provider.

The Scarsdale Public School District (SPSD) met the selection criteria and was chosen as the pilot site. A leader from the SPSPD coordinated the district's internal effort to use the methodology. This individual was responsible for planning and budget management within the SPSPD and recognized the value of using the K-12 Risk Methodology in justifying technology expenditures. To assure that appropriate individuals were selected for participation on the analysis team, the SPSPD leader

reviewed the description for this research, specifically part of Chapter 1 of this document, to gain an understanding of the importance of pilot site participation and the responsibilities of the selected analysis team. Selected members of the teaching staff, curriculum design staff, technology staff, and administrative staff were chosen for the SPSD analysis team. In addition, these individuals had good communication skills and were interested in improving information security. The analysis team committed one day a week for eight weeks to learn and complete the evaluation to meet the specified timeframe.

This researcher conducted four guidance sessions with the analysis team to familiarize participants with the methodology and review progress as the team performed the methodology workshops. For Guidance Session 1, this researcher provided an introduction to the issues of security risk management and an overview of the K-12 Risk Management analysis team activities. The PowerPoint slide presentation *Managing the Risk of Internet Connectivity* (Woody, 2003) introduced the need for security risk management in K-12 schools and school districts to SPSD analysis team participants. During the remainder of the first session, the K-12 Risk Methodology materials used by analysis team members in their execution of the methodology were reviewed. Those materials consisted of worksheets and step-by-step instructional guidelines for each activity to be performed. The activities were grouped by the phase in which they occur. Appendix D contains a detailed description of each activity within each phase and the title of each worksheet to be used by the analysis team to document the results of each activity.

For Guidance Session 2, this researcher returned to the SPSD when the analysis team completed the required activities and outputs of Phase 1: Organizational View. During this session, the analysis team presented the results for the following: assets, areas of concern, security requirements, current protection strategy survey results, critical assets, and threats to critical assets. As a consequence of questions from analysis team members about the use of the Organizational View worksheets for constructing threat trees, two separate workshops were required: Guidance Sessions 2A and 2B. During Guidance Session 2A, analysis team questions were resolved. During Guidance Session 2B, the SPSD analysis team presented the completed worksheets for Phase 1. Work to be addressed in Phase 2: Technology View was also discussed during Guidance Session 2B. Phase 2 of the methodology is performed only if individuals knowledgeable in the use of vulnerability assessment tools are available. The SPSD analysis team determined that Phase 2 could not be performed because the school district did not have access to the necessary expertise and could not purchase the expertise from external sources within the time constraints of the pilot. As a consequence, the analysis team moved forward with Phase 3: Security Strategy and Planning.

During Guidance Session 3 the results of the Phase 3 activities were reviewed. Analysis team members presented their completed worksheets and answered the following questions:

- How has the use of the methodology expanded your understanding of K-12 school information security issues?
- How have the plans for actions, mitigations, and protection strategies that were developed with the methodology addressed school district security concerns?

- How has use of the methodology prepared you to address information technology (IT) decisions and security issues in your school district?

Guidance Review Sessions 2B and 3 identified additional K-12 school and school district issues that were not included in the initial tailoring of the methodology. In addition to responding to questions about the value of the methodology, SPSD analysis team participants were asked for ideas about how to improve the methodology and its effectiveness for K-12 schools and school districts in general. Members of the SPSD analysis team provided information about the following:

- Gaps and issues not addressed by the tailored methodology that should be incorporated,
- Areas where the structure and format hindered the SPSD analysis team's use of the materials, and
- Recommended revisions that would improve the usability of the materials.

All K-12 Risk Methodology outputs created during the SPSD use of the tailored methodology remained the property of the SPSD and were not part of the reported research results. This research focused on the methodology and its effectiveness for helping K-12 schools and school districts, and SPSD as a sample member of this domain, identify and address security risks through the application of a security risk assessment methodology.

Because of the wide variation in school size and technology capability among K-12 schools and school districts, an individual pilot site could not be considered a representative sample (K. Krueger, personal communication, February 21, 2003). To expand the review process to a broader audience, the tailored methodology was presented

for review and comment to a group of ten K-12 school officials, including school board members, technology directors, and superintendents. Reviewers were members of the Consortium for School Networking (CoSN), a national non-profit organization that draws its members from K-12 schools and school districts across the country. In preparation for this review, the CoSN assembled a Security Focus Group (SFG). Participants in that group included three individuals serving on the CoSN executive board who previously expressed interest in K-12 school security and several attendees at the K-12 School Networking Conference 2003 in Arlington, VA who signed up to participate in the SFG through self-selection. The SFG participants met once at the conference to review the same PowerPoint slide presentation used as an introduction for the SPSD analysis team. Communication with SFG participants was coordinated through an assigned member of the CoSN executive board (S. Miller, personal communication, February 27, 2003).

After the SPSD finished using the K-12 Risk Methodology, changes recommended by analysis team participants were applied, and the updated version was released to SFG members for their review. In addition to suggestions and questions about specific methodology content, SFG participants were asked to respond to the following questions:

- How is the methodology applicable to your K-12 school or school district?
- Is the provided material sufficient for use in your K-12 school or school district?
- Has your concern about the K-12 school security issues increased, decreased, or remained unchanged based on review of the methodology?

## **Formats for Presenting Results**

Two products in Microsoft Word format were assembled from this research. The first product was the K-12 Risk Methodology based on the OCTAVE Methodology. That product consisted of worksheets and step-by-step instructions for completing process activities included in the security risk evaluation tailored for K-12 schools and school districts using the OCTAVE Approach (Alberts & Dorofee, 2002). Major segments of that first product are included in this report (Appendices E, F, G, and H) to illustrate specific tailoring actions applied to the methodology.

The second product was a report highlighting the shortcomings and value of the methodology as identified by the analysis team and CoSN Security Focus Group (SFG) participants. That second report incorporated the lessons learned from tailoring activities, and pilot and expert reviews of the methodology. The information in that report is described in Chapter 4 and Appendix L of this document.

## **Outcomes**

This research raised the awareness of security risk management issues for analysis team participants at the selected pilot site. In addition, K-12 schools and school districts represented by the participants in the SFG review group reported increased awareness. Copies of the two products of this research were provided for use by CoSN members. Since a high level of interest in information security was expressed by its members as a result of this research, the CoSN announced an initiative for cyber-security in the K-12 schools and school districts. That initiative involved establishing funding for development and dissemination of an assemblage of training and tools tailored to K-12

school security (<http://securedistrict.cosn.org/>). The focus of the U.S. on information security underscores the importance of a viable methodology to address the risk of K-12 school and school district Internet connectivity nationwide and contributes to the involvement of school administrators in addressing issues and challenges in that area (CIPB, 2002).

As a consequence of this investigation, a security plan developed by the analysis team using the K-12 Risk Methodology was implemented at the SPSD. That plan included action items for immediate needs, mitigation procedures for protecting critical information assets, and a protection strategy for long-term security management of critical technology resources within the K-12 school district. Team participants who implement security plans are expected to become advocates for security risk management and assist the CoSN in helping other K-12 schools and school districts benefit from the use of this methodology. The SPSD analysis team participated in the announcement of the CoSN cyber-security initiative at the National School Boards Association's (NSBA's) 2003 Technology Plus Learning Conference, October 2003, in Anaheim, CA.

Based on statements from SFG reviewers during the initial meeting at the 2003 K-12 School Networking Conference, participants in the review process gained an understanding of the issues of security risk management that are applicable to the K-12 school environment. They are expected to seek additional information about security issues and support the planned CoSN initiative for applying security risk management within their K-12 schools and school districts (S. Miller, personal communication, February 27, 2003).

Through the application of a tailored risk methodology based on the OCTAVE Methodology, the benefits of knowing the best practices assembled by SEI researchers and incorporated into the OCTAVE Methodology through the OCTAVE Catalog of Practices are available to K-12 schools and school districts. In the long term, through the use of a consistent structure across a range of K-12 schools and school districts, patterns for the best practices suited to the unique security risks and needs of the K-12 environment are expected to emerge. Those patterns can then be incorporated into an enhanced K-12 Risk Methodology (K. Krueger, personal communication, August 26, 2003).

Researchers at the SEI continue to refine the OCTAVE Methodology based on feedback from entities tailoring the methodology to unique needs such as K-12 schools and school districts. This researcher used the methodology publicly available (<http://www.cert.org/octave>) as of December 15, 2002 for this investigation. Refinements to the OCTAVE Methodology since that time should be reviewed and incorporated into the K-12 Risk Methodology in future investigations to further enhance the process if those refinements are appropriate for the needs of K-12 schools and school districts.

## **Resources Used**

This researcher gained an understanding of the OCTAVE Methodology through training and helping government agencies apply the methodology. An understanding of the K-12 school environment has been gained through experience and document reviews to successfully build a tailored version for use by the selected pilot site. As a member of

the Networked Survivable Systems technical staff at the SEI, this investigator worked for two years with the SEI researchers who developed the OCTAVE Methodology and is qualified to teach the OCTAVE Methodology. Moreover, this researcher worked with licensed OCTAVE Methodology transition partners to develop automated tools for the U.S. Department of Defense medical community to support the expanded use of the methodology. In addition, this researcher has 25 years of application and systems design experience with large complex environments for Yale University, Land and Legal Records for West Chester County of New York, and the Administration for Children's Services of New York City.

Knowledge of challenges and solutions available within the field of information security protection was needed to conduct this investigation. Some of that expertise was incorporated within the OCTAVE Methodology template worksheets and instructional guidance that served as a basis for the K-12 Risk Methodology. This researcher completed the SANS Institute Global Information Assurance Certification (GIAC) for GIAC Security Essentials (GSEC) in January 2002 to better understand the focus and limitations of the OCTAVE Methodology for security risk management.

A pilot site with a student body and teaching staff that serviced the full age range of K-12 students was required. Also, participants from a range of areas within the K-12 domain including teaching and technology support were required. The burden of regulatory reporting imposed by NCLB requirements was given as the reason for several possible sites declining to participate in this process. The Scarsdale Public School District in Scarsdale, New York met the selection criteria and volunteered to be the pilot site. The director of instructional computing led the analysis team in this effort. Selected

analysis team participants at the pilot site contributed time to learn the steps of the methodology, apply it to their school environment, and identify areas where the methodology failed to meet their needs.

A resource to help identify experts in the K-12 school technology environment who could perform the follow-up review of the material used in the pilot was critical to the completion of this research. The executive director of the Consortium for School Networking (CoSN) accepted this responsibility in exchange for use of the resulting methodology content by Consortium members.

### **Reliability and Validity**

Within the field of security risk management, no general measurements that can define reliability and validity for K-12 schools and school districts are identified (Pethia, 2003). Much of the field expertise is contextual in nature and focused on defining responses to vulnerabilities within the infrastructure as each vulnerability is identified (Allen et al., 2000). Validation is provided through a series of peer reviews performed by individuals working within security management who address a wide range of security challenges (Allen & Sledge, 2002). The tailored methodology for K-12 schools and school districts was subjected to reviews by the pilot site and K-12 experts. This process is similar to validation steps used for the OCTAVE Methodology (Alberts et al., 2000).

Organizations that used the OCTAVE Methodology realized benefits that included an increased awareness of applicable security issues and recognition that security must address threats that have a real impact on the capabilities of the entities to

perform critical functions effectively. This same benefit was expressed by the pilot site and SFG K-12 reviewers in their use of the K-12 Risk Methodology.

Another benefit of using the OCTAVE Methodology was the development of a common understanding of the value of security risk management as a consequence of understanding the real risks across the entity (Alberts & Dorofee, 2002). As noted in the feedback from the K-12 pilot site participants (see Appendix L), use of the K-12 Risk Methodology provided similar benefits though improved decision-making that grew from a shared understanding of the need for security and an increased awareness of the risks if security issues were not addressed.

## **Summary**

The OCTAVE Methodology was selected for use in this research effort as a basis for introducing security risk management into K-12 schools and school districts. Purchase, training, and licensing costs were not required for its use. Tailoring options were available for addressing the unique requirements of K-12 schools and school districts. Because the methodology is used by a sufficiently broad range of organizations, it is considered appropriate for addressing the security issues of K-12 schools and school districts that use Internet connectivity.

Based on an initial analysis of the methodology and confirmation with the SEI researchers who developed the methodology, the OCTAVE Methodology was tailored to fit the unique needs of the K-12 environment as identified by this researcher. Requirements identified in the literature review were applied to the OCTAVE Methodology to build a tailored version referred to as the K-12 Risk Methodology. This

researcher had sufficient training and support from the SEI to construct an appropriately tailored methodology. The OCTAVE Criteria were used to confirm completeness of the tailored methodology as required for consistency with the OCTAVE Approach (Alberts & Dorofee, 2001a). A school district was identified to apply the tailored methodology for initial validation. In addition, experts in the K-12 school domain were assembled to review the methodology and provide further validation of its applicability to K-12 schools and school districts.

## Chapter 4

### Results

#### **Data and Process Analysis**

This research consisted of four major segments: (1) building the tailored methodology; (2) validating the tailoring process; (3) testing the tailored methodology in a K-12 school district; and (4) reviewing the tailored methodology with K-12 school representatives. The specific actions of each segment are summarized below to provide sufficient information to support the findings and allow for replication as needed by other researchers.

#### *Building the Tailored Methodology*

This researcher worked independently to build the K-12 Risk Methodology by applying in-place tailoring options from the OCTAVE Methodology. Based on an initial review of those options best suited to incorporate unique K-12 school security risk issues as described in Chapter 3, the following changes were applied:

- Expanded security practices to incorporate those important for K-12 schools but missing from the OCTAVE Catalog of Practices (see Appendix A);
- Restructured data collection activities used in assembling an organizational view in Phase 1: Organizational View to incorporate an expanded K-12 Catalog of

Practices and include modifications to accommodate a distributed organizational structure typical of K-12 schools and school districts, as opposed to the hierarchical structure embedded in the OCTAVE Methodology;

- Augmented the threat profile content in Phase 1 to incorporate the unique characteristics of information asset users within the K-12 environment that differ from the delineations assumed by the OCTAVE Methodology;
- Restructured Phase 3 worksheets to allow for evaluation criteria different from the OCTAVE Methodology and incorporate the expanded K-12 Catalog of Practices for mitigation and protection strategy considerations; and
- Adjusted terminology within the methodology to remove the use of terms such as business and customer that were irrelevant in the K-12 environment and renumbered the materials to accommodate the restructured segments and worksheets.

The application of each selected change to the methodology is described in detail in the remainder of this section.

### Expanding the OCTAVE Catalog of Practices

The OCTAVE Catalog of Practices is divided into two major groups: strategic practices and operational practices. Practices within each group were determined to be relevant to K-12 schools and school districts by this researcher and remained in the expanded K-12 Catalog of Practices for the tailored methodology. This decision was based on the number of security risks identified in the literature review for this investigation that were addressed by security practices currently included in the OCTAVE Catalog of Practices. A table containing 49 entries of security risks, associated

outcomes, and the security practice that mitigates each risk is provided in Appendix B. Those practices mapped to existing practice areas within the OCTAVE Catalog of Practices. Security practices that are not in the OCTAVE Catalog of Practices but were needed to address K-12 school and school district security risks (39 in all) were inserted into the K-12 Catalog of Practices. Appendix A lists those practices. Those practices were organized into four general categories that are referenced as educational security practices in this document:

1. Content-blocking. This category includes practices that filter for pornography and restrict access to inappropriate activities for minors.
2. Structured access. This category includes practices for equipment sharing, privacy, and access rights within an environment that requires extensive resource sharing.
3. Regulatory compliance. This category includes state regulations as well as federal ones including the Children's Online Privacy Protection Act (COPPA), Family Educational Rights and Privacy Act (FERPA), Protection of Pupil Rights Amendment (PPRA), No Child Left Behind (NCLB) Act, and the USA PATRIOT Act.
4. Acceptable educational use. This category includes restrictions against commercial use of educational facilities, ethics, individual responsibilities for using the infrastructure, and limitations for monitoring.

By keeping educational practices in a separate group within the expanded K-12 Catalog of Practices, K-12 school and school district personnel could determine how well they were addressing risk with respect to general security practices and how well they were

meeting specific educational security practices. Appendix D includes the revised structure of the OCTAVE Catalog of Practices as it was tailored for the K-12 Risk Methodology.

### Restructuring Data Collection

Data collection activities within Phase 1: Organizational View of the OCTAVE Methodology are grouped into three processes that include similar activities, but are structured to address three levels of an organization: (1) senior management, (2) operational management, and (3) staff. Staff includes information technology (IT) representatives (Alberts & Dorofee, 2002). The main difference among these processes is the worksheet survey form used to define the current security practices considered relevant to each level of the organization. Within the staff level, technical staff and organizational staff also use different survey instruments. These distinctions have no relevance to K-12 schools and school districts (TSSA, 2001). Moreover, it is unclear whether any selected subset of current security practices would be sufficiently universal to all K-12 schools and school districts to be meaningful. Instead of creating separate processes used by specific K-12 groups with an uncertain knowledge of relevance, a single data-gathering process was built by collapsing all the separate activities into a single process. This unified process was applied once by the pilot site, but could be used repeatedly with varying participants for broader information gathering in Phase 1.

The data collection process for the K-12 Risk Methodology can be applied through two distinct approaches that can be used separately or together depending on school requirements. In the first approach, each member of the analysis team addresses each activity in the data collection process independently. A group discussion is the next

step to refine the perspective, share knowledge, and construct an agreed group output.

This approach was used by the Scarsdale Public School District analysis team during the validation of the K-12 Risk Methodology.

The second approach is similar to using of data collection within the OCTAVE Methodology. For this approach, the analysis team conducts a facilitated workshop with a carefully selected group or groups of participants that represent one or more important segments of the K-12 school or school district. The workshop can be repeated for multiple groups based on the size and complexity of the sponsoring entity. Following the workshops, the analysis team consolidates data from all workshops and uses that data to construct an agreed group output. Participants in the facilitated workshop can include teachers such as computer science instructors, parents, students at varying ages and technology skill levels, and external support groups. These individuals are not required to join the analysis team and commit to the full amount of time required for methodology deployment. That flexibility allows the methodology to be applied to individual schools, school districts, and statewide programs with minimal adjustments.

Within Phase 1 of the OCTAVE Methodology, the OCTAVE Catalog of Practices is applied through a set of practice survey worksheets used to gather information about the current security practices (Alberts & Dorofee, 2002). To incorporate the expanded K-12 Catalog of Practices, some tailoring of the survey worksheets was required. That expanded catalog includes strategic and operational practices from the OCTAVE Catalog of Practices. Two surveys from the OCTAVE Methodology that incorporate these practices, specifically, the Current General Security Practices Survey and the Current IT Security Practices Survey, were maintained unchanged in the K-12 Risk Methodology

(Alberts & Dorofee, 2001c). An additional survey was required to include educational security practices. The Current Educational Security Survey was modeled from the strategic and operational worksheets to gather information on current educational practices (see Appendix F for the Current Education Security Survey). The questions in this survey reflect the practices identified in Appendix A. These practices were incorporated into the expanded catalog of practices for the K-12 Risk Methodology.

When assembling survey results from a range of participants into a consolidated group response, the OCTAVE Methodology recommends a summative approach to survey responses. Consolidated survey results reflect a count of each response to each survey question (Alberts & Dorofee, 2002). For a small group or wide range of participant groups with varying levels of expertise, an evenly weighted assembly of responses is not appropriate. The K-12 Risk Methodology provides for a group procedure that enables the analysis team to use the survey responses from all participants in constructing a consolidated perspective. Survey responses from a range of sources can be weighted differently based on the known expertise of the participants. This approach builds an analysis team perspective on the current state of security practices within the K-12 school or school district based on a qualitative assessment of survey responses. Appendix G includes a Security Practices Summary that provides a combined survey worksheet with results grouped by practice area. The analysis team can assure that all perspectives are considered through team discussions even when the participant count is skewed to selected participant groups.

## Augmenting Threat Profile Content

Threats within the OCTAVE Methodology are divided into those posed by outsiders who do not have legitimate access to information assets and insiders who have legitimate access but may not use it appropriately at all times (Alberts & Dorofee, 2002). This division is based on the SEI findings that entities must apply different mitigation and protection strategies, depending on the origin of the threat (Alberts & Dorofee, 2001c). The OCTAVE Methodology assumes insiders are employees of the entity and outsiders are non-employees. Within K-12 schools and school districts, there are gray areas when applying the insider and outsider designation. Students can function as either, depending on the information asset considered. Moreover, the role of parents in accessing student information is changing. Vendors may own and manage assets on behalf of the K-12 school or school district (AWS, 2002). Areas of concern identified about an asset within the assessment process must be linked to specific school positions such as student or teacher to establish appropriate relevancy. To make this distinction more explicit in the K-12 Risk Methodology, a field for specifying the positions with legitimate access and those without it was added to the asset description area of the Asset Profile Workbook. The Asset Profile Workbook is a set of worksheets completed for each critical asset selected by an analysis team within an application of the methodology. In that workbook, the analysis team records relevant information about a critical asset selected for evaluation. Instructions for the analysis team in defining insiders and outsiders were added to the guidelines for activity A1.3 to accommodate the Workbook change. See Appendix E for a description of that activity. The roles of insider and outsider are

specified to insure that all participants in defining threats to an information asset share a similar perspective of who should and should not be permitted access to the asset.

### Restructuring Phase 3 Worksheets

Three worksheets are used for the analysis process within Phase 3 of the OCTAVE Methodology: (1) Evaluation Criteria, (2) Protection Strategy for Strategic Practices, and (3) Protection Strategy for Operational Practices. Each worksheet required adjustments to appropriately incorporate the needs of K-12 schools and school districts. The impact categories on the Evaluation Criteria worksheet represent major concern areas for an entity in the event of a security breach. The OCTAVE Methodology incorporates the following basic areas of concern based on work with U.S. medical and manufacturing organizations: reputation or customer confidence; life or health of customers; productivity; fines or legal penalties; and financial impact. The research of Norris, Soloway, and Sullivan (2002), in evaluating the impact of technology within the classroom, identified the following categories of impact as appropriate evaluation criteria for K-12 schools and school districts: regulatory compliance; classroom planning and curriculum effectiveness; life, health, and safety of students, teachers, and staff; student performance on standardized tests and evaluations; family and community support; school and district administration support; teacher preparation and technical support; and other. The Evaluation Criteria worksheet was modified for use in the K-12 Risk Methodology to reflect the recommendations of Norris et al.

OCTAVE Catalog of Practice categories are incorporated into Phase 3: Security Strategy and Planning. Those categories form the structure of the Protection Strategy for Strategic Practices worksheet and the Protection Strategy for Operational Practices

worksheet. Those worksheets provide a series of questions for each practice area to be used in the analysis. To appropriately incorporate the educational practices (added into the OCTAVE Catalog of Practices for the K-12 Risk Methodology as described previously in this document) the worksheets for Phase 3 activities were augmented with a Protection Strategy for Educational Practices worksheet (see Appendix H). Although closely following the format of the other worksheets used in assembling the protection strategy, that worksheet emphasizes the educational planning practices instead of strategic or operational practices.

### Review of Terminology

The OCTAVE Methodology consists of 1,800 pages divided into 18 volumes. Those volumes include a range of additional material such as technical reports and background information relevant to individuals with an extensive background in information security management but overwhelming to a group attempting to learn the rudiments of a new topic area (Alberts & Dorofee, 2002). To minimize the volume of information imposed on the K-12 pilot group participants, only content relevant to the K-12 Risk Methodology was included, and the text was condensed into a single manual. That manual included step-by-step instructions for each activity of the K-12 Risk Methodology grouped by phase. In addition, the manual included a section containing all worksheets used once within the methodology activities. Worksheets that applied to each critical asset and required multiple uses within the methodology activities were assembled within a separate section in the manual for ease of duplication. Throughout the manual, the terms business and enterprise were changed to the general term school.

Also, the term department was changed to unit. (The complete table of contents for the K-12 Risk Methodology manual is included in Appendix E.)

### *Validation of the Tailored Methodology*

This researcher conducted a review of each adjustment to methodology activities and worksheets with SEI researchers who developed the OCTAVE Methodology. In addition, as described in Chapter 3 of this report, the tailored methodology was reviewed to assure conformance with the OCTAVE Approach. Conformance was measured through a review using the OCTAVE Criteria, which are divided into ten principles describing the methodology approach and fifteen attributes that identify how the principles must be applied within the methodology. A detailed description of the principles and attributes and an explanation of the relationships between them are provided in Chapter 3.

Validating conformance of the K-12 Risk Methodology to the OCTAVE Criteria required a review of guidance instructions to assure the appropriate application of each principle and attribute (Alberts & Dorofee, 2001a). Also, validation of the principles and attributes based on the use of the methodology provided assurance of the appropriate application of the guidance. Based on this review, the K-12 Risk Methodology conformed to the principles and attributes of the OCTAVE Criteria. For each principle, the table in Appendix I provides the following validation data:

- In the column labeled Principle the name of the principle;
- In the column labeled Applied assurance that the principle was applied;
- In the column labeled When a definition of when the principle was applied;

- In the column labeled Applied to Methodology Guidance a description of the application of the principle to the guidance; and
- In the column labeled Applied by Pilot Site a description of use of the principle by the pilot site.

All rows in the Applied column contained the yes, indicating successful conformance.

The When column contained one of two options:

- Unchanged, which means guidance and use in the tailored version were the same as in the OCTAVE Methodology.
- Tailored, which means the guidance and use were modified for the K-12 Risk Methodology, and the mechanisms for maintaining conformance are described the columns labeled Applied to Methodology Guidance and Applied by Pilot Site.

The K-12 Risk Methodology conforms to the attributes of the OCTAVE Criteria.

For each attribute, the table in Appendix J provides the following validation data:

- In the column labeled Attribute the name of the attribute;
- In the column labeled Applied an assurance that the attribute was applied;
- In the column labeled When a definition of when the attribute was applied;
- In the column labeled Applied to Methodology Guidance a description of the application of the attribute to the guidance; and
- In the column labeled Applied by Pilot Site a description of the use of the attribute by the pilot site.

The values used in the Applied and When columns are the same as described above for the table of principles in Appendix I.

### *Testing in a K-12 School District*

Selection requirements identified in Chapter 3 were met by the selected entity. Based on the information assembled from the school handbooks for each grade level, interviews with the site coordinator and technical staff, this researcher applied the selection criteria defined in Chapter 3 of this report and determined that the Scarsdale Public School District (SPSD) met requirements for selection as the pilot site. Four individuals were chosen by the site coordinator to join him as analysis team participants. This researcher participated in four meetings with the analysis team, specifically referenced as Guidance Session 1, Guidance Session 2A, Guidance Session 2B, and Guidance Session 3. An overview of those sessions is included in this section. In addition, the SPSPD analysis team met multiple times between each of the four sessions to complete assigned segments of the methodology.

The SPSPD consists of one high-school with an enrollment of 1,200 students, one middle school with an enrollment of 900 students, and five elementary schools with enrollments in each ranging from 350 to 500 students. Every school has at least one computer laboratory for use by every grade level. In addition to the laboratory, every classroom has active computer connections for instructional use by teachers. A fiber optic Gigabit Ethernet wide-area network (WAN) interlinks all the schools. The Technical Services staff, with third-party support, coordinates district-based technology activities. Internet Service Provider (ISP) services, firewall operations, and content filtering are handled by a third party. Students do not assist with network administration, but they do assist with classroom audiovisual support. Students attend regularly scheduled computer classes at all grade levels. The computer education curriculum

includes courses addressing the following topic areas: computer operations; publishing and presentation; creativity and design; problem-solving; and research. All students, starting in kindergarten, are provided with access to the school network.

### Initial Meeting

This researcher met with the technology coordinator to review requirements for consideration as a pilot site for this investigation and confirmed that participants from the SPSD could invest the required time to validate the K-12 Risk Methodology. A copy of the first chapter of this document was provided to the SPSD coordinator prior to the initial meeting. The coordinator shared the document with the technical services supervisor and network specialist responsible for the general supervision of the school district network infrastructure. During this initial meeting, the following topics and concepts were reviewed:

- Hardware, software, network infrastructure components and services, and technical support from a system administration perspective;
- Security policy, procedures, practices, monitoring efforts, and problems; and
- Distinctive features of the K-12 population including student enrollment demographics, teaching and administrative staff demographics, technology use and support in the school curriculum.

Each participant expressed a strong interest in the risk assessment process. No previous risk or vulnerability evaluation work had been conducted by the participants because of cost constraints. At the coordinator's suggestion, the analysis team included participants in this initial meeting who represented the curriculum and technology areas. In addition, an administrative manager and assistant manager joined the analysis team.

The technology coordinator was the analysis team leader and handled all communication between this investigator and the analysis team. Analysis team participants worked together on other school district initiatives and shared information extensively.

### Guidance Session 1

This researcher initiated Guidance Session 1 with a presentation using materials from a CoSN conference presentation in February 2003 (Woody, 2003). In addition, a brief description of the K-12 Risk Methodology, and an overview of the expanded OCTAVE Catalog of Practices were provided. The SPSD analysis team determined that the assessment would focus on the instructional technology, the administrative systems, and Internet usage by the school district. For the validation process of the tailored methodology, the analysis team selected one critical asset from each of the focus areas to use in the methodology workshops. The student folder repository was selected to represent instructional technology; the payroll database represented administrative systems, and the ISP represented Internet usage.

### Guidance Session 2A

The second meeting between this researcher and the SPSD analysis team was scheduled to occur when the analysis team completed the Phase 1 activities. However, team participants were unable to apply the generic threat trees to the selected assets. Analysis team participants reported difficulty in identifying threats that had not actually materialized. This researcher determined the participants were applying a reactive approach to the analysis and had not considered the impact of potential threats. By adjusting the original sequence of activities and developing evaluation criteria prior to

using the generic threat trees in Phase 1 instead of waiting until Phase 3, the analysis team was able to proceed with the assessment activities.

To address the evaluation criteria, the analysis team chose to adjust the impact areas provided in the K-12 Risk Methodology. The team members identified impacts in terms of the highest priority for K-12 schools and school districts as follows:

- Required by a regulatory mandate;
- Led to an article on the front page of the local newspaper;
- Resulted in parents calling members of the school board with complaints;
- Affected the ability of teachers and students to meet their classroom schedule; and
- Interrupted online services especially Internet access.

As a result of the dependency of all work at the school district on electronic communication, a loss or interruption of online services was selected by the SPSD analysis team as the most critical impact, and the team decided to use that as the only evaluation criteria within the application of the methodology. The methodology allows for the selection of multiple evaluation criteria, and the analysis team's decision to focus on only one is unique. To apply the evaluation criteria to the selected threat paths and determine the importance of each possible threat, varying degrees of impact were established. The OCTAVE Methodology uses a qualitative scale of high, medium, and low. The analysis team established the levels of impact for interruption of online services as follows:

- A low impact would involve up to a half-day interruption.
- A medium impact would involve up to two days of interruption.
- A high impact would involve any interruption that lasted two or more days.

With defined evaluation criteria, the analysis team returned to the Phase 1 activity (A1.6) of defining threats to the selected assets using the generic threat trees worksheets in the Asset Profile Workbook. Those trees provided a template of potential threats that should be considered when analyzing an asset (Alberts & Dorofee, 2001b). The template, the same for both the K-12 Risk Methodology and the OCTAVE Methodology, groups threats into four categories based on the threat source or access path used to reach the asset:

- Human actors using network access;
- Human actors using physical access;
- System problems such as viruses, software defects, system crashes, and hardware defects; and
- Other problems outside of the entity's control such as power supply problems, telecommunications problems, and natural disasters.

Within each template group, asset threats are selected based on the following:

- An actor who can be categorized as an insider or outsider of the asset;
- A motive that can be deliberate or accidental, and only applies to human actor threat sources; and
- A security outcome that can be disclosure, modification, loss/destruction, or interruption.

These combinations are organized graphically into a tree structure. The template for Human Actors Using Network Access is provided in Appendix K for reference. Usually, a subset of the possible threats applies to an asset, and the selected paths appropriate to the asset are highlighted in the Asset Profile Workbook. However, the analysis team

found no means of eliminating any of the paths and so chose to include all of them for each critical asset.

### Guidance Session 2B

Instead of constructing a team output for each critical asset as described in the instructions, each SPSD team participant selected a single critical asset and individually assigned an impact value to all the possible generic threats for the critical asset using the single evaluation criterion established in Guidance Session 2A, specifically, loss or interruption of online services. Next, each risk in the Human Actors Using Network Access category for each critical asset was reviewed by the technology participants, and impact values were adjusted to reflect existing protection mechanisms that reduced the potential impact. Subsequently, all individual worksheets were discussed by the team, and impact values were adjusted to reflect a team result. Though the analysis team used a different sequence of steps, the results met the requirements for outputs of Phase 1: Organizational View.

The SPSD analysis team next considered the activities for Phase 2. This researcher provided a brief review of the skills required to address the Technological View. The technology participants confirmed that their school district had neither the necessary skills nor a means of acquiring external expertise within the required timeframe for the evaluation. Based on the lack of required expertise, the analysis team decided to bypass Phase 2. The interactions between the school district and the service provider were informal and undocumented. The technical supervisor accepted an action item to document future interactions and discuss the possibility of a future vulnerability evaluation of the school district infrastructure with third-party support. To initiate Phase

3: Security Strategy and Planning, the team discussed which critical asset risks would be carried forward for mitigation consideration and decided to consider only high impact risks.

### Guidance Session 3

The final session was scheduled when the SPSD analysis team completed Phase 3. The team selected three security practice areas for strategic improvement and developed a plan for initiating improvement in each selected area. Selected analysis team members were assigned responsibility for the detail planning and implementation of improvement activities. The three areas were chosen to address the high-impact risks to the critical assets. The coordinator for the analysis team presented the protection strategy and implementation plan to the Scarsdale District School Board as the product of the security risk assessment to obtain approval to address the remaining activities for security risk management beyond the planning steps provided in the K-12 Risk Methodology.

SPSD analysis team participants reported an increased awareness of security risks after completing the surveys in Phase 1. Participants also suggested that examples of the completed worksheets for K-12 schools would clarify some of the activity instructions for future K-12 school and school district users. Participants suggested the following two sequence changes within the methodology based on problems encountered in its use at the SPSD: (1) introduce action planning in the survey analysis activities of Phase 1 and (2) move the activity of creating evaluation criteria to Phase 1 prior to addressing the threat profiles.

The SPSD analysis team agreed that the methodology was effective because of the following characteristics:

- The developer of the methodology was available to provide initial guidance as well as follow-up visits. This guidance kept the team focused on the methodology.
- The methodology provided a structure for allowing the team to assess its school district's security practices and make specific recommendations for improvement.
- The methodology was not focused on specific technology products and could be applied to all areas of the school district.
- The methodology facilitated an examination of a wide range of security practices and the development of recommendations based on selected critical assets.
- The security review activities provided a means of viewing security information from multiple perspectives, enhancing the confidence level of the analysis team in planned improvements.

The SPSD analysis team coordinator (Gerald Crisi, personal communication, July 25, 2003) provided the following recommendations assembled from analysis team input to better fit the methodology to the needs of other K-12 schools and school districts:

- Provide a documented introduction to the methodology that highlights its value to K-12 schools and school districts.
- Stress the importance of completing the assessment before applying its results.

Participants at the SPSD considered implementing selected actions identified in Phase 1. Only one of the three security practice areas selected for mitigation in Phase 3 was identified in the earlier Phase 1 plan. Without completing the

methodology, the analysis team would have initiated actions to address lower priority risks without realizing the higher impact risks were not being considered. Survey responses were provided by all analysis team participants (see Appendix L). The individual evaluations supported the team summary.

This researcher facilitated a discussion with SPSD analysis team participants to identify additional issues after receiving the survey responses. The following recommendations for future uses of the tailored methodology were identified during that discussion:

- Schedule the introduction to the materials in multiple sessions to avoid overloading individuals who are new to the concepts of risk and security with too much information at once.
- Schedule analysis team working sessions closer together to carry learning from one step to the next. A great deal of review was needed to re-engage SPSD team members between sessions.
- Assemble worksheet information and notes from each meeting for distribution to each team member to improve information sharing since not everyone can attend each team meeting.
- Consider team conversations that result in shared knowledge among the members as a major value in using the methodology.

As a result of using the K-12 Risk Methodology, the SPSD analysis team participants reported the following outcomes:

- Individual team members initiated changes within their specific areas to improve procedures and accountability for security that had not been previously considered.
- The team members planned to meet quarterly to consider high-impact risks for other information assets and to expand the use of the methodology within the school district.
- Survey worksheets were administered to groups of teachers and students to evaluate perceptions of security throughout the school district.

#### *Review by K-12 School Representatives*

Because there is a wide variation of size and technology capability among K-12 schools and school districts, an individual pilot site could not be considered a representative sample (K. Krueger, personal communication, February 21, 2003). To expand the review process to a broader audience, the tailored methodology was presented for review and comment to a group of ten K-12 school officials representing nine states. Review participants were selected from the membership of the Consortium for School Networking (CoSN), a national non-profit organization that draws its members from K-12 schools and school districts across the country. In preparation for this review, the CoSN assembled a Security Focus Group (SFG). Participants in this group included three individuals serving on the CoSN executive board who previously expressed interest in K-12 school security and attendees at the K-12 School Networking Conference 2003 in Arlington, VA who signed up to participate in the SFG through self-selection. Each participant was responsible for a student body that ranged in size from 2,500 to 6.5 million. Participants described their positions as follows:

- Director of instructional media and technology,
- Chief information officer,
- Associate superintendent,
- Educator,
- Director of technology,
- Content director,
- Consultant,
- Executive director, and
- School board member.

The SFG met once at the conference to review the same PowerPoint slide presentation used as an introduction at the pilot site. Participants expressed the following reasons for their interest in the methodology: (1) security is complex because the use of technology in K-12 schools and school districts is controlled at the individual classroom and student level; (2) existing resources are not sufficient for performing a complete assessment; (3) K-12 schools and school districts must respond to conflicting mandates for security from parents and regulators.

Each SFG participant received a copy of the K-12 Risk Methodology guidelines and worksheets. Methodology changes identified by the SPSD analysis team required a reordering of the activity steps. However, to avoid confusion of two versions of the methodology with differing sequences, these recommendations were communicated to the SFG review participants verbally by the CoSN coordinator.

Following the review of the K-12 Risk Methodology, SFG participants were asked to complete a questionnaire. Seven participants representing six schools and

school districts responded. The questionnaire contained seven statements to which the SFG participant selected agree, disagree, or do not know responses.

The following summarizes the responses:

Statement	Agree	Disagree	Do not know	No response
My school or school district currently addresses security risk adequately.		6	1	
Information security is considered in new technology purchasing and implementation in my school or school district.		4	3	
My school or school district devotes time and resources to security issues on a regular basis.	3	3	1	
The K-12 Methodology presentation expanded my concern of security risk in my school or school district.	6	1		
The presentation was adequate to understand the purpose and scope of the K-12 Risk Methodology.	7			
The K-12 Risk Methodology is something I would consider recommending for my school or school district.	7			
My school or school district would need training and technology assistance to consider the K-12 Risk Methodology.	3	2	1	1

## Findings

As demonstrated by this investigation of the K-12 Risk Methodology including its use by the Scarsdale Public School District (SPSD), a risk management approach can be used by K-12 schools and school districts to improve the management of Internet security risks. In addition, the selected school district was able to self-direct its efforts in applying risk management using the K-12 Risk Methodology. By applying the methodology, the SPSD analysis team used risk analysis to identify high-impact security risks to critical information assets. Subsequently, that team used risk mitigation to define a protection strategy for addressing those security risks.

At the SPSD and during the expert review, participants initially focused on specific actions that could be resolved quickly until the impact of potential risks was clarified. The opportunity to focus on a few critical assets provided by the K-12 Risk Methodology instead of attempting an exhaustive review was cited as important by participants in both the SPSD validation and expert review. According to findings from this investigation, K-12 school and school district personnel have limited time to apply to tasks outside of the daily responsibilities of their jobs, and these individuals benefit from a process that helps define achievable results within a finite timeframe.

Regulatory compliance is a primary focus of K-12 school administrators. Reviews and audits are performed on a constant basis by local, state, and federal authorities. None of the regulatory or audit controls for K-12 schools and school districts mandate a security risk assessment. However, the growing visibility of problems related to technology use in colleges and universities, and the increased visibility of technology-related incidents in K-12 schools and school districts has motivated K-12 administrators to consider the value of a security risk assessment. By addressing security risk management, an analysis team is prepared to respond to oversight inquiry when an Internet security problem occurs in its community. This capability was validated when the town of Scarsdale's Internet capability was compromised during the SPSD methodology validation, and school district leaders were required to respond to questions from the Scarsdale District School Board about the school district's Internet risk.

Linking the K-12 Risk Methodology with the Technology Support Index (TSI) (<http://tsi.iste.org/techsupport>), an assessment tool for profiling the support programs of K-12 schools and school districts provided by the ISTE, was suggested by SPSD analysis

team participants. The TSI assessment identifies four areas: (1) equipment standards, (2) staffing and processes, (3) professional development, and (4) intelligent systems.

Although the TSI assessment is not mandatory, it is used by K-12 schools and school districts to justify resource allocations for technology. Within each TSI assessment area, practices for technology are identified, but security practices are not included. In addition, existing audit and regulatory requirements used by local, state, and federal agencies to evaluate technology in K-12 schools and school districts should be expanded to incorporate the appropriate emphasis on security management. Based on the report of the Exploring the Future of Learning (EFL) Spring 2003 Education Forum, educators respond when regulatory and audit requirements are instituted (Armstrong et al., 2003).

#### *Findings Specific to the Scarsdale Public School District (SPSD)*

Identifying information assets, security requirements, threats, evaluation criteria, impacts, and information security risks using the required worksheets within the K-12 Risk Methodology for documentation was time-consuming for analysis team participants. The provided written instructions were sufficient after an initial introductory guidance session. A K-12 school or school district learning the methodology would benefit from a case study that supplied solution worksheets using a K-12 school or school district example for use as a training tool. Examples for a hospital are provided with the OCTAVE Methodology (Alberts & Dorofee, 2002). Analysis team participants relied extensively on additional explanations provided by this researcher in applying the methodology, and compensating options for that individualized guidance are needed for broad use of the methodology to be feasible.

Technical personnel were not prepared to perform vulnerability evaluations at the SPSD. The constantly changing mix of equipment within the network prohibited the use of vulnerability tools that were equipment specific. The K-12 school district infrastructure in this investigation was complex, spanning many locations and blending a wide range of technology components. The need for a low-cost approach to technology support eliminated the usage of many of the available vulnerability evaluation tools. K-12 schools and school districts would benefit from the development of a shared pool of tools, training materials, tips, and techniques based on security practices successfully applied at other K-12 schools and school districts.

### *SFG Review Findings*

The SFG review group demonstrated a strong interest in the use of a security risk management methodology. The Health Insurance Portability Accountability Act (HIPAA) regulations for security that were issued in February 2003 and mandated a risk assessment intensified interest of this review group since many K-12 schools and school districts must comply with HIPAA regulations. Such regulations specifically designate privacy control of student information to the existing Family Educational Rights and Privacy Act (FERPA) regulations, thereby, increasing the visibility of the K-12 school's and school district's role in the privacy of each student's personal information.

Based on survey responses, only a portion of the participating K-12 schools and school districts would be able to address security risk without additional support and training. A means of providing a low-cost training option is needed for the broad application of the K-12 Risk Methodology in K-12 schools and school districts. Examples specific to the K-12 school environment and an introduction that helps an

entity understand the value of a risk assessment, the selection of an analysis team, and the establishment of an appropriate scope for an assessment can partially address the training requirement.

SFG participants identified a major security risk for K-12 schools and school districts that provide a technology learning environment and an administrative support environment within the same infrastructure. A means of identifying security practices that work well within the K-12 school domain and a mechanism for sharing these practices with participants as lessons learned can benefit K-12 schools and school districts with limited resources.

#### *K-12 Risk Methodology Structure and Use*

The addition of an introductory document to provide direction in the selection of an analysis team and the scoping of an assessment is needed for new users. Also, based on observations by this researcher, a flowchart to help the analysis team track where it is at any point in the process would be beneficial. This flowchart could serve as a constant reminder of the overall goal of the series of activities, thereby, keeping the analysis team on track. The guidelines provide a complete and detailed process for using the worksheets and developing a protection strategy.

Linkage of the risk assessment with existing audit and assessment tools already in use in K-12 schools and school districts, such as the TSI assessment, can help provide a way for administrators to coordinate risk assessment activities with existing workloads. The survey instruments from Phase 1: Organizational View can also be used for multiple purposes since these instruments are based on good security practices that are applicable to a range of K-12 school and school district audits and evaluations.

Based on the SPSD usage, a reordering of selected methodology steps is needed. By introducing the action list in Phase 1 instead of Phase 3, ideas generated in security discussions can be documented. By moving the development of evaluation criteria into an earlier position in the process, the analysis team will be better prepared to consider potential threats and, thereby, avoid shifting from planning into execution mode with each identified security need. However, the true measure of threats will not be realized until the criteria are applied to value the threats, which cannot be accomplished until the final steps in Phase 3.

Some terminology used within the K-12 Risk Methodology is not consistent with common usage in the K-12 school domain. This researcher addressed major inconsistencies as part of the tailoring effort. Examples specific to the K-12 school domain can help clarify the meanings of terms not used regularly within this domain. Importantly, a careful review by individuals closely involved in the K-12 school domain should be considered before broad deployment of the K-12 Risk Methodology is attempted to minimize questions and reduce potential confusion.

## **Summary of Results**

K-12 schools and school districts can apply security risk management using the K-12 Risk Methodology as confirmed by its application at the selected pilot school district and its review by a group of K-12 school experts. Constraints of time and resources hamper broader use unless K-12 schools and school districts are mandated to perform a risk assessment or recognize the value of performing a risk assessment based on the impact of network security problems. At a minimum, the use of pieces of the

methodology such as survey worksheets from Phase 1: Organizational View can provide a starting point for considering the security practices needed for Internet security in K-12 schools and school districts.

The K-12 Risk Methodology provides a low-cost approach to security risk management that incorporates sufficiently unique characteristics of K-12 schools and school districts to be highly effective. Training support, expanded introductory materials, and automated tools to help manage the information collected using the methodology can enhance adoption by improving the mechanisms for learning and using the K-12 Risk Methodology. The changing and uncertain regulatory climate combined with a lengthy budget and approval cycle for funding underscore the importance of planning for security risk management in K-12 schools and school districts. With the K-12 Risk Methodology, investment for security can be planned to focus limited resources on the greatest security risks.

K-12 schools and school districts cannot continue to rely on teachers to control security within the classroom when these individuals are provided with limited preparation. Problems stemming from the lack of appropriate monitoring can be expected to increase as student use of technology with Internet connectivity extends beyond classroom time. Students cannot be used as resource extensions without effective management and monitoring. K-12 schools and school districts have an opportunity to address information security risk within the context of what is appropriate to each entity before general mandates are legislated.

By monitoring issues relevant to higher education, K-12 schools and school districts have the opportunity to recognize potential security problems and plan

appropriate responses instead of reacting to a realized impact. This planning opportunity may not remain available for a long period of time since behavior patterns point to K-12 students closely following those of older students. The increased visibility of K-12 student involvement in worm, virus propagation, and other criminal Internet activities that jeopardize critical national infrastructure can be expected to be accompanied by efforts to control the environments that provide Internet access to those individuals.

K-12 schools and school districts should proactively seek to influence the technology solutions for security available for use in classrooms. A shared repository of effective security practices should be established that identifies security implementation requirements for widely used K-12 software and hardware. Shared training programs for security awareness and guidelines for the unique needs of K-12 schools and school districts can augment limited staff technical skills.

## Chapter 5

### Conclusion, Implications, Recommendations, and Summary

#### **Conclusion**

This research demonstrated that security risk management can be applied by K-12 schools and school districts to address the security risks of Internet connectivity. This research also demonstrated that increased understanding of the impacts of security risks for Internet connectivity is a sufficient motivator for K-12 school and school district administrators to identify ways to address risk mitigation.

Expanded awareness of security issues by stakeholders within K-12 schools and school districts benefits administrators, teachers, curriculum developers, infrastructure support staff, students, and parents. From a shared understanding of the security threats to the classroom and their potential impacts, planned approaches can be developed to take advantage of lower cost opportunities and existing capabilities. A planned and reasoned approach effectively counters expensive politically motivated reactions performed to appease the vocal discord that arises from a crisis. Given the susceptibility of Internet connectivity to increasingly harmful security events, expanded Internet connectivity for the classroom will lead to an increase of security challenges for K-12 administrators (Pethia, 2003). Without planned security management, reactive responses can leave K-12

schools and school districts vulnerable to repeated security occurrences whose root problems are unaddressed.

Not all stakeholders require the same level of awareness. K-12 administrators need to understand the impact of security issues and ways the K-12 school and school district can effectively address those issues. Teachers and parents need to be aware of the steps taken by the K-12 schools and school districts to address security risk. Teachers also need to understand and follow procedures for reporting problems and identifying new areas of risk that may appear as classroom technology use expands and changes. Students need to be aware of the K-12 school's and school district's focus on addressing security risk, appropriate behavior patterns, and the penalties and sanctions they will face if their behavior deviates outside of expected norms.

K-12 school and school district personnel must recognize that the introduction of technology into the classroom environment is accompanied by an unknown level of security risk that must be managed. Students cannot be viewed as replacement resources for skilled staff, and student involvement in technical support must be closely and effectively managed. By performing a security risk assessment using the K-12 Risk Methodology, school personnel gain an increased awareness of the security risks within the context of their domain. Within the assessment, participants identify the greatest risks so that mitigation efforts can be focused on the most critical challenges.

According to this research, K-12 school districts such as the Scarsdale Public School District (SPSD) lack the expertise to address vulnerability evaluations and security audits. A structured assessment process tailored to the K-12 school domain that provides a means for identifying and correcting technology vulnerabilities can enhance

security functions provided by current K-12 technology staff. However, it is important that K-12 schools and school districts do not rely solely on technology solutions. K-12 school and school district administrators must also address the strategic and educational security practices required in effective security risk management.

The K-12 Risk Methodology provides a low-cost solution that allows schools and school districts to approach the risk assessment activities over an extended period of time. General security practices incorporated into the K-12 Catalog of Practices provide an increased awareness of risk areas that K-12 school and school district personnel must consider and appropriate practices that should be applied at each entity. The K-12 Risk Methodology is a planning process that guides K-12 school personnel in assembling an information protection strategy. To realize the full benefit of security risk mitigation, school and school district personnel must execute the resulting plan.

## **Implications**

In the process of conducting this investigation, this researcher introduced a wide range of individuals within the K-12 school domain to issues of security risk. This researcher spoke at the following conferences and presented issues related to the need for security risk management in the K-12 school domain:

- Consortium for School Networking, CoSN K-12 Networking Conference, Arlington, Virginia, February 2003, a panel presentation titled *Meeting the Security Challenges of the Connected Schoolhouse*;
- Exploring the Future of Learning (EFL) Policy Forum, Washington, D.C., April 2003, a two-day facilitated discussion of invited participants to identify critical

educational challenges. This researcher proposed K-12 security needs in a presentation titled *The Security Challenges of the Internet*; and

- The FBI Infraguard of Pittsburgh hosted a one-day conference for K-12 school and school district administrators held at Duquesne University in Pittsburgh, PA, November 11, 2003. This researcher delivered a presentation titled *Addressing the Risk of Internet Connectivity for K-12*.

The Scarsdale Public School District (SPSD), the pilot site for this investigation, was selected by the National School Boards Association (NSBA) as one of the top five technology schools in the U.S., and participants from the analysis team shared their application of security risk management at the award presentation in October 2003 (<http://www.nsba.org>). In addition, the April 2003 issue of *School Planning & Management Magazine*, a publication for K-12 administrators, contained an article by Enderle (2003) titled “Are School Networks as Safe as We Think?” That article referenced this research effort and a cyber-security initiative established by the Consortium for School Networking (CoSN).

Based on its K-12 school and school district members’ need for help in managing security risks, the CoSN established a partnership for launching a new initiative called Cyber Security for the Digital District (<http://securedistrict.cosn.org>). That partnership involved the U.S. Department of Education (ED) and vendors that sell security tools and services within the K-12 school domain, such as Symantec and SurfControl. That initiative, which builds on this research, will develop a program to accomplish the following goals:

- Promote an awareness of technology security issues that must be considered in the K-12 schools and school districts.
- Identify K-12 school and school district best practices for information security that can be adopted as K-12 infrastructure standards and incorporated into training and tools that provide information about security options to network administrators.
- Promote the inclusion of digital-age ethics in the K-12 school curriculum.
- Show school decision makers and technology directors how to improve the security for systems that handle data collection, transmission, storage, retrieval, and distribution of sensitive information.
- Provide publications to the K-12 vendor community to clarify the needs of information security in products designated for the K-12 school and school district.

This researcher has no formal involvement with the funded project beyond supplying a copy of the K-12 Risk Methodology for use by CoSN members at the completion of this investigation.

Specific actions planned by the CoSN to address initiative goals include the following:

- A white paper to define security risk management issues in terms appropriate for K-12 school and school district administrators.
- Training programs for K-12 school and school district administrators in the application of the K-12 Risk Methodology.

- A survey of the security problems and practices in use within the K-12 schools and school districts to identify common problems and best practices.
- Enhancement of the usability of the K-12 Risk Methodology by addressing formatting issues identified by participants in this research and automating the assembly of required documentation.
- The creation of a Web site for school network administrators to serve as a resource for K-12 security information, training, and vulnerability assessment tools. That site will parallel other CoSN leadership initiatives including Taking Total Cost of Ownership to the Classroom (<http://www.classroomtco.org>) and Safeguarding the Wired Schoolhouse (<http://www.safewiredschools.org>).
- A presentation of Web interactive conferences with participation from network leaders, security consultants, and vendor representatives to debate information security issues in K-12 schools and school districts.
- Tools developed or assembled to help local education leaders and network administrators analyze and address K-12 information security risks and infrastructure vulnerabilities.
- Workshops, conference presentations, and online courses developed to clarify information security issues, demonstrate available tools, and feature action plans for K-12 personnel.
- Articles published in magazines and professional journals, such as *School Planning and Management Magazine*, that target K-12 school board members, administrators, and other K-12 decision makers to broadly distribute ideas and

increase awareness of information security solutions for K-12 schools and school districts.

## **Recommendations**

The educational results of current legislative efforts to insert technology into the classroom are unclear (Armstrong & Casement, 2000). Measurements that will become available through further educational research should be applied to evaluate security practices in use by K-12 schools and school districts. Measurement of the effectiveness of security practices will provide a means for a stronger alignment of applied security actions with the educational mission.

A single methodology approach for security risk management was considered in this research. Comparing the results of using the K-12 Risk Methodology with other widely used risk assessment methodologies, such as the Facilitated Risk Analysis Process (FRAP) or the Information Protection Assessment Kit (IPAK), could enhance the options available to K-12 schools and school districts in addressing a security risk assessment. Such a comparison could also expand the understanding of security risk analysis in the K-12 school domain.

Issues related to security awareness and training should be reinforced consistently for students beginning at the kindergarten level and continually as they progress through all levels of the educational system. Research should be conducted to determine whether the consistent application of good security practices that are structured using a uniform risk methodology and adopted by K-12 schools and school districts improves the adoption of ethical behavior by K-12 learners.

Advanced training of K-12 technical staff in security for new technology areas should be considered. If a K-12 school or school district initiates a program that introduces hardware and software new to its technology infrastructure, such as a wireless network, funding should be allocated for security. That funding should be spent on training technical support personnel about security problems and practices for the new technology. Funding should also support implementation of monitoring capabilities to support an acceptable level of security risk. This process may require a change in the way new technology is implemented in the K-12 classroom.

Based on feedback from the SPSD analysis team and responses to the survey questionnaire by K-12 school and school district representatives in the Security Focus Group (SFG), K-12 schools have not planned for security management. This lack of planning is exhibited in the K-12 administrative responses to security incidents reported in the news media. Harsh responses such as felony charges and jail sentences for student incidents of adjusting or deleting files (Legon, 2003) indicate an administrative reaction instead of a planned response. Only 19% of K-12 schools and school districts have acceptable use policies (AUPs) (NSBF, 2002a). If appropriate ethical training for students is not applied and appropriate use policies are not in place and enforced, security breaches from K-12 students can be expected to increase.

Higher education institutions are bound by many of the same federal regulatory requirements such as FERPA and HIPAA that apply to K-12 schools and school districts. Similar security risks are applicable to both domains because both types of institutions must support teaching, learning, and administration (Salomon et al., 2003). Findings from the application of security risk management in K-12 schools can serve as a foundation for

the application of security risk management in community colleges, colleges, and universities.

K-12 schools and school districts have the opportunity to prepare for problems with technology use by monitoring what is occurring in college and university environments and learning from the experiences of those institutions. As technology use in K-12 classrooms increases, administrators must assume that the associated security management problems experienced in higher education will also appear in their K-12 schools and school districts. K-12 administrators have an opportunity to establish appropriate authority figures knowledgeable in technology to reinforce appropriate behavior patterns for students (Verton, 2002), but doing so will require an expanded investment in technical staff resources that are documented as under-funded (NSBF, 2002B).

As a large consumer group of technology, K-12 schools and school districts have an opportunity to influence technology developers to provide more secure products. Technology currently in use in K-12 classrooms is not secure by design, and vendors serving the K-12 market must be encouraged to improve the functionality of available security (Armstrong et al., 2003). Expanded technical training of teachers and staff responsible for technology management in K-12 schools and school districts is a necessity (Schwartau, 2001). It is no longer sufficient for self-taught teachers and volunteers to be assigned full responsibility for the technical infrastructure when Internet connectivity is added to it (Kenneally, 2002).

## Summary

This researcher introduced security risk management concepts and a structured methodology for evaluating security risk to K-12 administrators. The OCTAVE Methodology was tailored to incorporate security practices and measurements unique to K-12 schools and school districts, and was successfully applied by the Scarsdale Public School District (SPSD) to identify and plan for security risk mitigation.

In contrast to medical, financial, and federal-government agencies, security risk management is not mandated for K-12 schools and school districts. Based on responses from participants of the SPSD analysis team and the SFG review group, this investigator determined that limited awareness of security issues resulting from Internet connectivity and the lack of funding available to maintain technology security are major causes of poor security management within K-12 schools and school districts. K-12 administrators, staff, and teachers would benefit from the application of a structured methodology tailored to the needs of the K-12 domain. In addition, K-12 administrators would benefit from a formalized means of sharing security practices and security technology expertise. Through the CoSN and its planned distribution of the K-12 Risk Methodology to its membership along with supplemental educational and technical support tools, low-cost security risk management processes can become available to individuals responsible for Internet connectivity in K-12 schools and school districts.

School administrators and teachers are pressured by potentially competing demands to improve minimum student learning as measured by the NCLB regulations and to apply technology within the K-12 school and school district infrastructure as emphasized by the E-rate program. As a result, technology installed using E-rate funding

has not been consistently applied within the K-12 curriculum except by individual teachers with sufficient training and technical support to incorporate technology usage into their classrooms (Cuban, 2001). The lack of standard practices for technology training, support, and protection within the K-12 classroom has contributed to a lack of regard for technology security by teachers and school curriculum developers (TSSA, 2001). In contrast, technology dependency has increased within the administrative functions in K-12 schools and school districts where regulatory monitoring in response to the NCLB Act has forced extensive automation through external sources (AWS, 2002). In order to understand and address the security needs of this complex and changing technology environment, K-12 school and school district administrators can benefit from the planned approach to information asset identification, security requirement identification, and security threat identification and assessment provided by the K-12 Risk Methodology.

Educational oversight organizations such as the Department of Education (ED) have not recognized a responsibility for balancing the expanded reporting and data access requirements with appropriate security risk management requirements. In addition, K-12 school and school district administrators and school board members have not recognized their responsibility to evaluate the security risk of the technology infrastructure to establish acceptable use policies in the same manner as acceptable facility use and risks to student health and safety are evaluated and addressed.

Federal, state, and local regulators for K-12 schools and school districts must consider the importance of security risk management in the funding and monitoring of

K-12 school and school district technology use. The appropriate consideration of security for Internet-accessible information assets under the responsibility of each K-12 school and school district must become standard practice. The similarity of security risk management issues in K-12 schools and school districts to those of institutions of higher education has not been recognized by ED. Federal funding is available to colleges and universities to address security risk but not to K-12 schools and school districts.

Acceptable levels of security risk must be established and monitored to assure the privacy and protection of K-12 school and school district online resources.

Based on responses of the SFG, all participants in the technology decisions within K-12 schools and school districts require training to understand the security risk that is introduced through Internet access. In addition, training for K-12 decision-makers must support the development of an understanding of available measures for addressing security risk, implementation and maintenance mechanisms for continued security risk management, and resource levels needed to support effective security risk management. The lack of technology expertise for general technology support, which has been augmented by student assistance (NSBF, 2002a), is further aggravated by the lack of understanding of the need for security risk management by K-12 school and school district administrators.

The appropriate level of participation of students and teachers in K-12 school and school district technology support must be established. Involvement developed informally based on individually acquired technical expertise and technical staffing shortages has created potential security risk that must be addressed. Within each K-12 school and school district, a planned level of technology access for students and teachers

based on a security risk management plan that defines the appropriate level of participation for students and teachers can be established using the K-12 Risk Methodology.

Security risks within each K-12 school and school district are not well understood by those that plan and support the technology infrastructure. Content filtering has been the focus of concern for technology use based on regulatory mandate. This focus fails to address the wide range of risks to data quality and connectivity from both inside and outside sources that can occur through technology access. Based on the experience of SPSD, use of a well structured security risk methodology that includes the evaluation of current practice with a catalog of good security practices can enhance the concern for security by analysis participants.

K-12 administrators must recognize the complexity of the technology infrastructure available to support the teaching and administrative needs within each K-12 school and school district. Technical staff hired or contracted to provide support and maintenance must acquire sufficient skill to address technology infrastructure vulnerability evaluation and security monitoring. The skills needed to assist in performing the activities of Phase 2 in the K-12 Security Risk Methodology are critical to the ability of an entity to effectively recognize, resist, and recover from security events affecting the technology infrastructure. The technology support for the complex infrastructure implemented in K-12 schools and school districts must include in-depth security risk management expertise.

It is incumbent upon the leaders of K-12 schools and school districts, such as school board members and school administrators, to assign responsibility for security risk

management and monitor the effectiveness of applying security practices.

Inappropriately managed Internet connectivity can have serious impacts on the ability of K-12 schools and school districts to function effectively. This investigation has shown that use of the K-12 Risk Methodology can aid K-12 schools and school districts in addressing security risk management for Internet connectivity.

## Appendix A

## Security Practices Unique to K-12

School Context	Security Risk	Consequence	Security Practice	Reference
Access to quality content must be funded by someone.	Payment for technology access will be required without advertising dollars and may replace book purchases for libraries.	Learning may be jeopardized if appropriate content quality standards are not imposed.	Content blocking	ALA, 1999
Search engines are based on key words provided by supplier. They cannot be equated with library books that are selected.	Library materials are not readily available on the Internet. Quality does not always fit into the appropriate educational segment for learning.	Learning may be jeopardized if reliance on digital technology replaces paper books too soon.	Acceptable educational use	ALA, 1999
Placement of Internet in learning must be defined. Only small segment of world information is digitized.	Level of availability will be skewed to those with greater technology access.	Digital divide may impact educational capabilities of those with less access to technology.	Acceptable educational use	ALA, 1999
Means for identifying acceptable and unacceptable Web sites is needed.	Total reliance on generalized software is not realistic based on the limitations of the technology.	By providing means for human oversight & including local requirements (defined by parents and local authorities) the school can provide a better overall result.	Content blocking	Chapin, 1999
Extended use of specific portals instead of general searches to focus student learning can standardize availability of content.	Portals are restricted to a subset of content and not always maintained consistently (e.g., science [ <a href="http://www.enc.org">http://www.enc.org</a> ], math [ <a href="http://forum.swarthmore.edu">http://forum.swarthmore.edu</a> ], language arts [ <a href="http://www.eserver.org">http://www.eserver.org</a> ]).	Provides controlled environment without arbitrary limitations imposed by the technology, but may exclude content critical to specific learning	Content blocking and structured access	Chapin, 1999
Establish bookmark file to focus student activity and provide consistent content access.	Providing a consistent student interface that is repeatable across multiple class visits	Establishes a baseline that can be maintained between multiple users for the same equipment but requires technology resources to establish and maintain	Content blocking and structured access	Chapin, 1999

## Security Practices Unique to K-12 (continued)

School Context	Security Risk	Consequence	Security Practice	Reference
Web-based utilities can establish a means for classroom collaboration and sharing of files using free Web products.	Systems must be established that can appropriately control what is shared and with whom. Access must be controlled and maintained.	Techniques of sharing can be compromised to allow outsiders to see and change the contents inappropriately.	Acceptable educational use	Bell, 2001
Students should be protected from inappropriate content.	Parents, teachers, and students need to know the limitations of the blocking capabilities of the school.	Poorly educated users will react to problems as technology failings when they do not understand the limits of implemented choices. Education of the parents in adopted processes shows due diligence.	Content blocking	NSBF, 2002b
Parental guides for limiting child's use of Internet and monitoring sites are important	Failure to consider parental wishes when controlling Internet connectivity may lead to adverse publicity.	Verification that parental interests are considered shows recognition of parent's role in defining access for the child.	Acceptable educational use	NSBF, 2002b
High cost of connectivity may require outsourcing, sharing of resources across multiple school districts, or sharing with libraries or corporate environments.	Establishing an Internet service provider to cut costs and provide extensive software to students at low cost	Requires collective buying such as statewide to establish sufficient volume for cost effective technology purchasing; requires tight administration of access to meet the restrictions applied by software provider licensing and appropriate isolation of content for each group sharing the resource base	Acceptable educational use	Brewin, 2001
Chat rooms provide inappropriate meeting grounds for children and harmful elements.	A Web site that provides daily tips to promote online safety is <a href="http://www.chatdanger.com">http://www.chatdanger.com</a> which claims 80,000 visitors.	Children must be educated in the risks of technology use as well as its value; parents and teachers must know where to locate information to help them in the technology management of children.	Content blocking and acceptable educational use	Brooke, 2001

## Security Practices Unique to K-12 (continued)

<b>School Context</b>	<b>Security Risk</b>	<b>Consequence</b>	<b>Security Practice</b>	<b>Reference</b>
COPPA compliance requires carefully controlled private information collected on children. This regulation applies to all children under the age of 13.	COPPA regulations require conspicuous posting of privacy policy and verifiable parental permission for all data collected. Actions must match posted policy. Parents must have a means to revoke consent. Security and integrity of the collected data must be assured.	Compliance failures are prosecuted by FTC, and schools share in the liability if violations occur using school connectivity.	Regulatory compliance	Cannon, 2001
COPPA personal data must be protected if collected online.	First and last name, physical address, email address, screen name, other online identifiers, telephone number, and social security number must be protected. Cookies and other persistent electronic location identifiers are considered personal data.	School choices for connectivity management may violate COPPA compliance without careful review.	Regulatory compliance	Cannon, 2001
Safe-harbor status is available from COPPA.	Submission of site information to FTC for registration requires special controls and proof of compliance.	Registration as a safe-harbor provides validation of compliance.	Regulatory compliance	Cannon, 2001
Typing skills must be taught to children to make use of keyboard input mechanisms. Curriculum planning must establish a point in time when this skill is required.	Repetitive stress injuries are a high risk when work spaces are not tailored to incorporate ergonomic considerations of small and growing bodies.	The school may incur liability for excessive technology interaction of children at too early an age without proper consideration of the desks, chairs, posture, and other factors that contribute to maintaining healthy bodies.	Acceptable educational use	Biersdorfer, 1999
Are Internet-facilitated learning experiences being provided?	A definition of learning experience must be established to assure proper use of all types of access. Internet connectivity is only one portion of the social context necessary for learning from this media.	Internet connectivity may continue to be custodial in nature without proper incorporation into the learning environment.	Acceptable educational use	Bruckman, 2002
Exploration of the capabilities of the digital learning environment are still underway.	Peer-to-peer relationships and communications with outside experts have been identified as effective learning models but require extensive connectivity.	Is this level of access cost justified? How will this level of access be managed so as not to disrupt other modes? Is the cost of control too high?	Acceptable educational use	Bruckman, 2002

## Security Practices Unique to K-12 (continued)

School Context	Security Risk	Consequence	Security Practice	Reference
Should technology use be linked with test scores and student performance?	Existing metrics for evaluating success of an application may not be appropriate.	Funding sources have used poverty as a primary driver for technology need based on the assumption that the lowest performers need the greatest technology access.	Acceptable educational use	Schulte & Keating, 2001
Number of "student suspended" days was identified as a metric for educational interest.	Gains in state mastery test gains identified as increased with computer installation.	Cost of technology does not include sufficient levels of assurance for quality use. Teacher training seen as key to making gains. (Cost is greater than equipment and software.)	Acceptable educational use	Davis, 2000
Teachers who understand and use technology as a new means of communication can gain student involvement.	Students reluctant to communicate in class have been known to participant online in class discussions.	Removal of the prejudices that visibility adds to the communication can be beneficial.	Acceptable educational use and structured access	Chamberlin, 2001
Asynchronous communication can provide broader availability.	Requires different mode of communication and instructor thinking	Rules of engagement need to be established or the access path will be abused.	Acceptable educational use	Chamberlin, 2001
Immediate grading and analysis facilities promote immediate feedback.	Requires specific technical tools and individual student access to execute	Requires greater management to provide a view of performance over time and assurance of privacy of each participant	Acceptable educational use	Chamberlin, 2001
Federal regulation must be included as appropriate.	Expanded regulatory oversight with the Goals 2000: Educate America Act and Elementary and Secondary Education Act (ESEA)	Title I, Title II, Title III, Title IV, Title VI compliance may add to data needs and expand potential for abuse.	Regulatory compliance	Chambers et al., 2000
State and local regulation must be included as appropriate.	Standards, assessments, curricula, teacher preparation, and professional development must include technology considerations.	Funding sources are requiring measurements of success that expand data collection and control (e.g., NCLB).	Regulatory compliance	(Chambers et al., 2000)

## Security Practices Unique to K-12 (continued)

School Context	Security Risk	Consequence	Security Practice	Reference
Marketers are disguising advertising as educational content to capture youth spending.	Evaluation mechanisms for vendor-supplied materials are not standardized and may not consider the consequences of alternate content usage.	"Free" equipment may not be usable because of the control aspects used by the supplier.	Acceptable educational use	Colkin, 2001
Compliance with Americans with Disabilities Act must be provided.	Technology is frequently a support mechanism through the use of adaptive technology.	Technology solutions for disability divide may not be workable or may compromise student learning if not managed properly.	Structured access	Cunningham, 2000
Children must be taught the value of computers and of things other than computers.	Human interactions are identified as an area that is being lost with computer use especially for younger children.	Balanced curriculum must incorporate both computer use and human interaction with peers and teachers.	Acceptable educational use	Davis, 2000
Controlled access to content is available through simulated Internet.	Technology is applied inappropriately and content is controlled excessively within a limited closed environment.	EKIDS by Silvertech Inc. is an example of a closed environment that is considered safe for children, but it is unclear if it addresses learning needs.	Acceptable educational use	Davis, 2000
Policies, quality of available materials, and availability of consistent connectivity limit computer classroom use.	Goals for technology use in the classroom are unclear. Expectations of each stakeholder are not being met, causing frustrations.	Administrative support and teaching tools are not sufficiently consistent for classroom reliance.	Acceptable educational use	Sarkar, 2002
Content filtering must be applied appropriately to provide effective blocking of undesirable material with minimum impact on access to appropriate material.	Filtering best practices should be applied to the selection and implementation processes. Choices for filtering must reflect the planned use of the Internet for instruction and research.	Mechanisms to override the filtering must be available to allow choice to overcome limitations of the technology.	Content blocking	Balkin et al., 1999
Use of technology in the classroom changes the manner in which assignments are approached.	Formal and consistent structure cannot be assumed to exist with Internet materials, and each class use will vary.	Teachers must change their expectations and approach to materials to match the environment of the Internet.	Acceptable educational use	NETS, 2002

## Security Practices Unique to K-12 (continued)

School Context	Security Risk	Consequence	Security Practice	Reference
Use of E-Rate funding requires monitoring of effective use of technology.	Reporting is required to the Schools and Libraries Division (SLD) of the Universal Service Administration Company (USAC) of the Federal Communications Commission (FCC).	Schools must develop a technology plan that specifies incorporation of technology into curricula.	Acceptable educational use and regulatory compliance	ED, 2000b
Copyright restrictions on digital materials are in flux.	Control of use of digital materials is complicated by the changing regulatory environment.	Students and teachers must be educated in the restrictions that apply to copyright materials. Violations can put the school programs at risk.	Acceptable educational use and regulatory compliance	Gaunt, 2002
Expectations in the use of technology vary by region and economic level of school districts.	Appropriate use of technology must be linked to the local characteristics of Internet users.	Gauging local interest and value is a continuously changing effort.	Acceptable educational use	GAO, 2001
Funding for technology and ongoing support is dependent on goals shared with the public.	Experience in other projects, such as public transportation, shows that including public opinion within the planning can greatly improve acceptance.	Establishing shared goals can benefit the acceptance of limitation choices. Expectations must be controlled carefully to avoid additional regulatory oversight.	Acceptable educational use	Meyer, 2000
Choices of technology must match the learning needs of the classroom.	Teaching needs must drive the selection of appropriate technology.	A shared forum for identification of needs and evaluation of technology that incorporates planned use is needed.	Acceptable educational use	Sonwalker, 2001
Written permission is required from parents for release of any child education information or from the child when reaching age 18.	Regulations such as Family Educational Rights and Privacy Act (FERPA) and Protection of Pupil Rights Amendment (PPRA) apply privacy restrictions to use and disclosure of student personal information.	Directory information may be disclosed without consent, but parents must be notified with an option to exclude their child's data.	Regulatory compliance	ED, 2002a and ED, 2002b
Parents have the right to inspect all survey instruments that are used to collect data from children.	2001 education bill addresses indirect use of data collected for educational purposes from third parties and sold to others.	Failure to comply places the school at risk if collected information is used improperly.	Regulatory compliance	EPIC, 2003

## Appendix B

### K-12 Security Practices Consistent With OCTAVE Catalog of Practices

<b>School Context</b>	<b>Security Risk</b>	<b>Consequence</b>	<b>Security Practice</b>	<b>Reference</b>
Tracing physical location of machine	Physical location of equipment can be traced with data provided from a Web site.	Child can be located by sources that may do harm.	Security management	Moad, 2001
Enhance the educational opportunities but minimize the entertainment functions.	Vendors are providing content but not always supporting the educational needs of students.	Learning is disturbed by inappropriate content, and behavior is influenced inappropriately.	Security policies and regulations	ALA, 1999
Children's personal information must be protected from applications collecting private information inappropriately.	Widely used school applications (e.g., Café Terminal the online cafeteria payment system by Comalex, Inc) collect inappropriate data in violation of the COPPA.	Schools using applications that collect inappropriate information will be penalized.	Security management	<a href="http://www.comalex.com">http://www.comalex.com</a>
Acceptable use policy should be linked to filtering mechanisms in use, and parents should be notified of the policy restrictions imposed by the school.	Appropriate notification of parents is needed in all actions.	Informed parents will raise concerns within school channels instead of attacking educational efforts.	Security policies and regulations	Chapin, 1999
Monitoring of log files collected by a browser, filter, or proxy Web server can identify acceptable usage problems.	AUP enforcement and a means for updating filtering processes to maintain currency are required for effective enforcement.	Established rules must be enforced, or they will be ignored.	Security management	Chapin, 1999
Shared machines provide access to private information through caching, browser history file, personal bookmarks, and cookies.	Allows students using the same equipment to see and plagiarize what others students are doing (privacy invasion).	Establish specific start-up and shutdown procedures that limit reliance on individual actions and remove personal information between uses.	Information technology security	Chapin, 1999

## K-12 Security Practices Consistent With OCTAVE Catalog of Practices (continued)

School Context	Security Risk	Consequence	Security Practice	Reference
Desktop security can be impacted by actions of the user.	Access to infected email and acceptance of cookies can compromise user privacy and device software.	Internet access can adversely impact the desktop, rendering it unusable. Restrictions on what the user is allowed to do and what functions are automated must be considered.	Information technology security	Chapin, 1999
Outbound text filters can be used to block personal information in chat rooms, emails, and Web forms.	Technology is only partially effective. Requires links with AUP and training of individuals in acceptable use	Validation of acceptable activities is needed. Will chat and peer-to-peer be allowed? Will email be available?	Information technology security	Chapin, 1999
Training is required for educational use of tools.	Technology will not help if users are not knowledgeable in the use of the available tools.	Resources to address proper training of teachers, aides, and students must be considered.	Security awareness and training	Strauss, 2002
Teachers require training in specific equipment and capabilities of school.	Proper use of facilities, protection of passwords, and protection mechanisms in place must be part of standard teacher/aide training.	Reliance on teachers when they are not properly trained is ineffective and will subject the students to potential harm.	Security awareness and training	Strauss, 2002
Control of access to private student information is needed.	Assurance is needed that access to student personal information is limited to caregivers and teachers.	Information availability must be balanced with effective authorization and authentication mechanisms. Control of access must define and limit who can view and change data.	Information technology security	O'Toole, 2002
Lockdown of machines to avoid unanticipated compromise is needed.	Physical and software control is needed to avoid unexpected software changes.	Physical control of the machine can allow complete compromise of all standardized limitations.	Physical security	O'Toole, 2002

## K-12 Security Practices Consistent With OCTAVE Catalog of Practices (continued)

School Context	Security Risk	Consequence	Security Practice	Reference
Means for identifying inappropriate behavior on the system is needed.	Mechanisms must be in place to control who can view and adjust information logs.	Monitoring is required to assure compliance. Access to monitoring information must be controlled, or violators will remove the evidence.	Information technology security	Mackenzie & Goldman, 2000
Mechanism for enforcement of violations must be delineated clearly.	Who is the enforcement agent – students, teachers, or administrators?	All participants must be aware of who is monitoring and why.	Security management	Mackenzie & Goldman, 2000
Mechanisms are needed to limit traffic on network.	How much remote access will be provided to parents, teachers, students, or community access? Remote access for students and teachers traveling?	The establishment of priorities for critical applications and the prioritization of classroom needs over casual use may be required to assure asset protection.	Security policies and regulations	Mackenzie & Goldman, 2000
Are those accessing the network tested before access is granted to validate comprehension of AUP and other training?	Confirmation that AUP has been read and understood is needed.	Confirmation of knowledge of AUP provides greater leverage in enforcement.	Security management	Mackenzie & Goldman, 2000
Formal procedures exist for establishing computer abuse, reporting problems, and adjudicating violations.	Greater compliance is expected with assurance of consistency and knowledge in advance of processes.	Procedures require the identification of problems and resources for problem resolution.	Information technology security	Mackenzie & Goldman, 2000
Procedures for handling computer violations include identification of when police are to be notified	Potential abuses include sexual harassment, spam to mailing lists, forging mail, sniffing the network, port scans, cracking passwords, commercial use of the network	Recognition of problems that extend outside of the control of school administration and how they are to be addressed must be established in advance of the situation.	Security management	Mackenzie & Goldman, 2000
Clear definition of what constitutes resources under control of the school	Restrictions of inappropriate behavior require clear definitions of acceptable use.	Appropriate use must be defined in advance of providing access, and use must be monitored.	Security management	Mackenzie & Goldman, 2000

## K-12 Security Practices Consistent With OCTAVE Catalog of Practices (continued)

School Context	Security Risk	Consequence	Security Practice	Reference
Handling of chain mail and pyramid schemes – potential for mail storms with class lists	Inappropriate structuring of internal technology use can lead to internal denial of service.	Teacher and technology support training is required to learn how to recognize and respond to potential problems in advance.	Information technology security	Mackenzie & Goldman, 2000
Do mechanisms exist for tracking specific actions back to specific individuals for redress?	How will shared devices be evaluated? With logon usage to identify who is using machines, how can sharing of access passwords be prevented?	Monitoring of individual actions requires individual identification.	Information technology security	Mackenzie & Goldman, 2000
Education is needed for students and teachers on copyright restrictions. Limitations for educational material are based on licensing agreements.	How can the potential for selling access to illegal materials be managed? How can processes such as scanning be limited to legitimate purposes?	Policies and procedures are needed.	Security policies and regulation	Mackenzie & Goldman, 2000
Implementation of available technology standards is needed to prevent known problems.	Due diligence requires attention to known technology vulnerabilities (e.g., SANS 20 highest security holes).	Resources needed to apply all known corrections can be high. Consider must be given to the value of standardized installations.	Information technology security	Mackenzie & Goldman, 2000
What is an appropriate education of systems administrators?	Formal training, informal training, sharing of problems with other sites?	Consider the need for training technical support in security issues.	Information technology security	Mackenzie & Goldman, 2000
Who can add machines to the network? How are they controlled? Can personal machines of students, faculty, or parents be added to the network?	Control of illegal Web sites and machines using illegal access to enhance capabilities inappropriately is needed.	The level of control for machines inserted into the network will define the level of security possible.	Security policies and regulations	EDUCAUSE, 2002

## K-12 Security Practices Consistent With OCTAVE Catalog of Practices (continued)

School Context	Security Risk	Consequence	Security Practice	Reference
Do individuals set up their own passwords or are they assigned?	Easily guessed passwords provide an opening to the network for anyone.	Passwords that are too hard to remember require greater support assistance.	Security management	Verton, 2002
What forum exists for raising and evaluating security issues? Does this include technical, admin, and teachers?	Shared forum to identify problems before they are widespread will enhance response without increased cost.	Communication among all participants in the organization is needed for effective security.	Security management	EDUCAUSE, 2002
All users of the network are educated as to security threats and prevention options.	Student, teacher, and administrator access should be dependent on the level of training completed.	Failure to require training for network use will allow users to make mistakes that harm the infrastructure through ignorance.	Security awareness and training	Lesniak, 2002
Anti-virus software is available, used, and updated on all levels of connectivity (desktop/laptop, server, network).	Protection of the infrastructure from externally introduced malicious software is needed.	Protection may be required at multiple levels, especially with mobile devices.	Information technology security	Lesniak, 2002
Are patch levels of all software maintained to acceptable currency? Who defines acceptable?	By not applying patches, the software remains vulnerable to compromise through a known opening.	Patch application is resource intensive and time-consuming. Many applications may be disabled when changes for which they were not validated are applied.	Information technology security	Lesniak, 2002
Someone is assigned the responsibility for environment security and monitors the available knowledge sources (e.g., SANS, CERT/CC).	Identified vulnerabilities are doubling annually. Support of effective connectivity requires constant vigilance.	Resources must be assigned to monitor and support the infrastructure.	Information technology security	Lesniak, 2002
Unneeded services are removed, and passwords are controlled for all devices.	The greater the level of resources on a device, the greater the level of required support.	If services are available but not used, there is a tendency to limit support to reduce resource usage. Known problems are not fixed leaving vulnerabilities available for exploit.	Information technology security	Lesniak, 2002

## K-12 Security Practices Consistent With OCTAVE Catalog of Practices (continued)

School Context	Security Risk	Consequence	Security Practice	Reference
Response team exists and knows what to do if the network has problems.	When the infrastructure is compromised, resources must know what to do to address the problem quickly and restore connectivity.	Security attacks will happen, and methods for addressing them are required.	Information technology security	Lesniak, 2002
How are technically skilled students identified and managed?	Without appropriate monitoring, the students who know the network can become inside threats.	Reliance on resources that are not contractually obligated to maintain an effective environment poses a high risk with very little recourse in the event of problems.	Information technology security	Verton, 2002
How are ethical issues of copyright and intellectual property being communicated to network users?	What enforcement options exist for these issues, regardless of the media?	School resources will be placed at risk if users of these resources do not take their responsibilities seriously.	Security policies and regulations	Colkin, 2002
Biometrics devices represent a means of authentication that is easy to use and can be implemented without reading skills.	Passwords require a level of reading that may be above some of the K-12 school users.	Biometrics are more expensive to implement but more difficult to bypass.	Information technology security	Carr, 2001
Internet connectivity provides access to a broad range of non-educational opportunities.	Entertainment options consume bandwidth that is needed for other purposes.	Control of the use of available infrastructure resources requires restrictions to non-essential services.	Security management	Clark, 2001
Wireless connectivity provides flexibility for workspace and teaching locations.	Security for wireless connectivity is extremely limited.	Can wireless be limited to areas where functionality exceeds risk?	Information technology security	Cope & Brewin, 2000
Clear definitions of the level of privacy and what monitoring is being done must be communicated.	Employees and students anticipate privacy while using a computer. However, monitoring facilities allow administrators to see everything.	Infrastructure administrative capabilities must be severely restricted to minimize the risk of inappropriate use.	Security management	Cohen, 2000

## K-12 Security Practices Consistent With OCTAVE Catalog of Practices (continued)

School Context	Security Risk	Consequence	Security Practice	Reference
Communication of acceptable and unacceptable reuse of available digital material must be part of the teaching process.	Violation of copyright laws can be accomplished easily with current technology. Continuous reinforcement of appropriate use is needed.	Tools and their use can overwhelm students. Care must be taken in the construction of assignments to differentiate original work electronically from plagiarism.	Security policies and regulations	Clayton & Watkins, 2002
Internet access requires balancing of two requirements: keeping children safe and increasing student achievement.	Agreement on what is meant by safety and achievement is needed at each organization.	Policies and procedures must be consistent with local goals to facilitate achievement.	Security policies and regulations	NSBF, 2002b
Control of access and clarity of structure can be provided through the use of portals.	Development is required to build and support portals, but single sign-on and customization creates a simplified learning environment.	Development of a consistent approach for access and control across all classes can simplify administration and use.	Security policies and regulations	Eisler, 2000
Providing access though school infrastructure for equipment not owned and controlled by the school is needed.	The level of security available to be considered will be limited, based on the level of control participants are willing to accept.	Technology planning must be based on the connectivity decisions of participants.	Security policies and regulations	Norris & Soloway, 2001
Outsourcing technology support with insufficient control of vendor's decisions may compromise security.	Protection from pornography will not be available if outsourcing organizations are not applying consistent protection mechanisms.	Students can be exposed to content from shared vendor environments against planned policy.	Collaborative security management	Radcliff, 2001

## K-12 Security Practices Consistent With OCTAVE Catalog of Practices (continued)

School Context	Security Risk	Consequence	Security Practice	Reference
Access to email addresses and contact information linked with a school can compromise child safety.	Control of information unknowingly shared through outside access via the Internet can put a child at risk.	Schools must educate students about the value of keeping their network access private.	Information technology security	Rosencrance, 2002
Establishing curricula based on availability of specific Internet sources can be risky.	Web-based sources may not represent viable businesses, and materials may not be consistently available.	Web sources must be held to the same standards as other information sources to assure that appropriate educational standards are maintained.	Collaborative security management	Schulman, 2001
Volunteer sources and corporate donations must be evaluated, based on the organization's goals.	Limited availability and limited control of volunteers may mean additional support must be absorbed by the organization.	Volunteer sources must be held to the same security standards as other information resources.	Collaborative security management	Schneider, 1999
Introduction of technology requires inclusion of appropriate ethics for use of delivery media.	Appropriate use of content is not readily provided by the delivery mechanisms of technology.	Guidelines for use must be understood before access to technology is provided.	Security awareness and training	Colkin, 2002
Web site and Internet access policies should be highly visible for reference by students and parents.	Filtering, acceptable use enforcement, and data management practices should match posted information policies.	Consistency is required across all parts of the organization for effective management of information protection.	Security awareness and training	Chapin, 1999

## Appendix C

### Mapping OCTAVE Principles to Attributes (Alberts & Dorofee, 2001a)

<b>Principle</b>	<b>Attribute</b>
Self-direction	Analysis team, Augment analysis team skills
Adaptable measures	Catalog of Practices, Generic threat profiles, Catalog of Vulnerabilities
Defined process	Defined evaluation activities, Documented evaluation results, Evaluation scope
Foundation for a continuous process	Next steps, Catalog of Practices, Senior management participation
Forward-looking view	Focus on risk
Focus on the critical few	Evaluation scope, Focused activities
Integrated management	Organizational and technological issues, Organizational and information technology participation, Senior management participation
Open communication	Collaborative approach
Global perspective	Organizational technological issues, Organizational and information technology participation
Teamwork	Analysis team, Augment analysis team skills, Collaborative approach, Organizational and information technology participation

## Appendix D

### Catalog of Practices for K-12 Risk Methodology

- I. Strategic practice areas
  - a. Security awareness and training
  - b. Security strategy
  - c. Security management
  - d. Security policies and regulations
  - e. Collaborative security management
  - f. Contingency planning/disaster recovery
- II. Operational practice areas
  - a. Physical security
    - i. Physical security plans and procedures
    - ii. Monitoring and auditing physical security
  - b. Information technology security
    - i. System and network management
    - ii. System administration tools
    - iii. Monitoring and auditing information technology security
    - iv. Authentication and authorization
    - v. Vulnerability management
    - vi. Encryption
    - vii. Security architecture and design

## Catalog of Practices for K-12 Risk Methodology (continued)

### c. Staff security

- i. Incident management
- ii. General staff practices

## III. Educational practice areas

### a. Content blocking

- i. Filtering pornography
- ii. Blocking access to inappropriate activities
- iii. Monitoring to limit censorship

### b. Structured access management

- i. Privacy including the Family Educational Rights and Privacy Act (FERPA) and Protection of Pupil Rights Amendment (PPRA)
- ii. Resource sharing management
- iii. Access rights management

### c. Regulatory compliance

- i. Children's Online Privacy Protection Act (COPPA)
- ii. Copyright and licensing laws for digital media and the Technology Education and Copyright Harmonization (TEACH) Act for the educational use of electronic media
- iii. Federal and state reporting
- iv. Protection against criminal use of technology to violate state or federal law including the Computer Fraud and Abuse Act (CFAA), Electronic Communications Privacy Act (ECPA), and Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act

## Catalog of Practices for K-12 Risk Methodology (continued)

- d. Acceptable educational use
  - i. Participant's responsibilities (varies by age)
  - ii. Organizational responsibilities
  - iii. Ethics

## Appendix E

### Table of Contents for K-12 Methodology Instructional Guidance

<b>During Phase I</b>			
<b>Activity</b>		<b>Description</b>	<b>Worksheets</b>
A1.1	Identify Assets and Relative Priorities	Identify assets that are used by the organization. Then, select the most important assets to the organization and discuss their rationale for selecting them.	<i>Asset worksheet (W1.1)</i>
A1.2	Select Critical Assets	Identify assets that can have a large adverse impact on the organization if harmed.	<i>Asset Profile Workbook (one for each critical asset)</i>
A1.3	Identify Areas of Concern	Identify scenarios that threaten the most important assets, based on typical sources and outcomes of threats. Consider impacts to the organization for those scenarios.	<i>Areas of Concern worksheet (W1.2)</i> <i>Asset Profile Workbook</i>
A1.4	Identify Security Requirements for Most Important Assets	Identify the security requirements for the most important assets. Select the most important security requirement for each important asset.	<i>Asset Profile Workbook</i>
A1.5	Current Protection Strategy Practices and Organizational Vulnerabilities	Complete surveys to indicate which practices are currently followed by the organization's personnel, as well as ones which are not followed. After completing the survey, discuss specific issues from the survey in more detail.	<i>Current General Security Practices Survey (W1.3)</i> <i>Current Educational Security Survey (W1.4)</i> <i>Current IT Security Practices Survey (W1.5)</i> <i>Protection Strategy worksheet (W1.6)</i> <i>Security Practices Summary (W1.7)</i>
A1.6	Identify Threats to Critical Assets	Threats are identified from areas of concern mapped to structured profiles.	<i>Asset Profile Workbook</i>
A1.7	Identify Evaluation Criteria	The organization uses evaluation criteria for all activities. Areas of greatest impact must be identified and applied to security.	<i>Identify Evaluation Criteria (W1.8)</i>

## Table of Contents for K-12 Methodology Instructional Guidance (continued)

<b>During Phase 2 (Optional)</b>			
<b>Activity</b>		<b>Description</b>	<b>Worksheets</b>
A2.1	Identify Key Classes of Components	The analysis team establishes the system(s) of interest for each critical asset. The team then identifies the classes of components that are related to the system(s) of interest.	<i>Asset Profile Workbook</i>
A2.2	Identify Infrastructure Components to Examine	The analysis team selects specific components to evaluate. The system(s) of interest is automatically selected for evaluation. The team selects one or more infrastructure components from each key class to evaluate. In addition, the team also selects an approach and specific tools for evaluating vulnerabilities.	<i>Asset Profile Workbook</i>
A2.3	Run Vulnerability Evaluation Tools on Selected Infrastructure Components	The IT staff or external experts conduct the vulnerability evaluation. They are responsible for running the vulnerability evaluation tools and creating a vulnerability summary for each critical asset prior to the workshop.	N/A
A2.4	Review Technology Vulnerabilities and Summarize Results	The IT staff members or external experts who ran the vulnerability tool(s) present a vulnerability summary for each critical asset and interprets it for the analysis team. Each vulnerability summary is reviewed and refined if appropriate.	<i>Asset Profile Workbook</i>

Table of Contents for K-12 Methodology Instructional Guidance (continued)

<b>During Phase 3</b>			
<b>Activity</b>		<b>Description</b>	<b>Worksheets</b>
A3.1	Identify the Impact of Threats to Critical Assets	The analysis team defines impact descriptions for threat outcomes (disclosure, modification, loss, destruction, and interruption). The impact description is a narrative statement that describes how a threat ultimately affects the organization's mission. The combination of a threat and the resulting impact to the organization defines the risk to the organization.	<i>Asset Profile Workbook</i>
A3.2	Create Risk Evaluation Criteria	The analysis team creates evaluation criteria that will be used to evaluate the risks to the organization. Evaluation criteria define what constitutes a high, medium, and low impact.	<i>Asset Profile Workbook</i>
A3.3	Evaluate the Impact of Threats to Critical Assets	The analysis team reviews each risk and assigns it an impact measure (high, medium, or low).	<i>Asset Profile Workbook</i>
A3.4	Create Mitigation Plans	Create risk mitigation plans for each critical asset. A mitigation plan defines the activities required to mitigate the risk/threats to the critical assets.	<i>Asset Profile Workbook</i> <i>Security Practices Summary worksheet (1.7)</i>
A3.5	Create Action Plans	Create action plans for near-term activities that are needed to address security areas but do not require specialized training, policy changes, or other longer term steps.	<i>Asset Profile Workbook</i> <i>Security Practices Summary worksheet (1.7)</i>
A3.6	Create Organization Protection Strategy	Create a protection strategy for the organization. That strategy defines how the organization will enable, initiate, implement, and maintain its internal security.	<i>Security Practices Summary worksheet (1.7)</i> <i>Asset Profile Workbooks</i>

## Appendix F

### Current Educational Security Practices Survey Worksheet

<b>Current Educational Security Practices Survey</b>			
<b>Practice</b>	<b>How is this practice used by your organization?</b>		
<b>Content Blocking</b>			
Policies and procedures for applying content blocking have been defined, and installed software and hardware filtering tools are set up to implement the policy.	Yes	No	Unknown
Content blocking is applied appropriately to all available services (Internet, email, chat services, and applications) and to all types of communication mechanisms available within the organization (desktop, laptop, wireless, cell phone, remote devices of varying kinds, etc.) based on policies that may vary by role and student age.	Yes	No	Unknown
A reporting and correction capability exists for problems with content blocking. Default settings for filtering can be adjusted to correct problems. The responsibilities for problem identification and problem correction have been assigned within the organization.	Yes	No	Unknown
Content-blocking policies and procedures are in accordance with parental and local definitions of inappropriate content (Internet sites, spam, ads, solicitations, etc.).	Yes	No	Unknown
Digital content used for education is evaluated for validity and appropriateness to assure that learning is not jeopardized through the use of online content instead of textbooks. This process is consistently applied to all learning materials.	Yes	No	Unknown
Content-blocking mechanisms are sufficiently supported to maintain a consistency as online content and capabilities expand.	Yes	No	Unknown
Purchase arrangements for technology, which includes vendor monitoring, are evaluated for consistency with content-blocking policies and procedures.	Yes	No	Unknown

## Current Educational Security Practices Survey Worksheet (continued)

<b>Current Educational Security Practices Survey (cont.)</b>			
<b>Practice</b>	<b>How is this practice used by your organization?</b>		
<b>Structured Access Management</b>			
Technology choices are matched to the needs of the technology participants.	Yes	No	Unknown
Mechanisms have been established to assure that individuals sharing equipment cannot infringe on the privacy of others using the same equipment.	Yes	No	Unknown
Shared content is available through the use of bookmark files, portals, and other structures that assure consistency without reliance on specific access devices.	Yes	No	Unknown
Policies and procedures for remote access to information are established and consistently managed. They include security considerations appropriate to the devices and applications involved.	Yes	No	Unknown
Technology access and availability is consistent with organizational policies for compliance with the Americans with Disabilities Act.	Yes	No	Unknown
Software- and equipment-selection processes include consideration for physical and online security throughout the useful life of the purchase.	Yes	No	Unknown
Implementers and monitors are aware of control mechanisms (physical and online), and mechanisms exist for the identification, reporting, and correction of problems throughout the useful life of the technology.	Yes	No	Unknown
<b>Regulatory Compliance – Children’s Online Privacy Protection Act (COPPA)</b>			
Controls are in place to assure that all private information for children under the age of 13 is not released without parental consent.	Yes	No	Unknown
Monitoring mechanisms are in place to assure that children cannot reach sites that do not appropriately apply COPPA restrictions in collecting information.	Yes	No	Unknown

## Current Educational Security Practices Survey Worksheet (continued)

Current Educational Security Practices Survey (cont.)			
Practice	Is this practice used by your organization?		
<b>Regulatory Compliance – COPPA (continued)</b>			
Safe-harbor status has been established internally, and sites approved as such have been identified for use by children under the age of 13.	Yes	No	Unknown
<b>Regulatory Compliance – Copyright and Licensing Laws</b>			
Appropriate use of digital materials is actively encouraged.	Yes	No	Unknown
Discussions of ethical behavior and definition of appropriate use occur on a regular basis at all levels of technology participants.	Yes	No	Unknown
Penalties for inappropriate behavior are understood as required by all levels of technology participants. Monitoring mechanisms are established appropriately.	Yes	No	Unknown
Validation mechanisms have been identified and are applied periodically to digital content to confirm appropriate licensing management.	Yes	No	Unknown
<b>Regulatory Compliance – Federal and State Reporting</b>			
Information collection to support mandated Federal reporting is defined and consistent with organization policies of privacy.	Yes	No	Unknown
Information distribution is handled in compliance with the Family Educational Rights and Privacy Act (FERPA) and the Protection of Pupil Rights Amendment (PPRA).	Yes	No	Unknown
Compliance requirements linked to standards, assessments, curricula, teacher preparation, and professional development are consistent with organizational policies and good practices for secure use and availability.	Yes	No	Unknown
Programs for inserting technology into the organization provide clear consideration for organizational policies and good practices for secure use and availability.	Yes	No	Unknown

## Current Educational Security Practices Survey Worksheet (continued)

<b>Current Educational Security Practices Survey (cont.)</b>			
<b>Practice</b>	<b>Is this practice used by your organization?</b>		
<b>Regulatory Compliance – Protection Against Criminal Use of Technology</b>			
Technology users are aware of the restrictions to external sites imposed by the Computer Fraud and Abuse Act (CFAA), Electronic Communications Privacy Act (ECPA) and Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act, and organizational use policy provides a means for enforcing these restrictions.	Yes	No	Unknown
Mechanisms are in place for identifying the inappropriate use of organization facilities with respect to generating potential harm to other sites, and the capability to identify violators and impose penalties on their actions is in place.	Yes	No	Unknown
Standards of conduct for individuals with technical skills and system access that would allow them to violate federal and state restrictions are clearly defined and enforced.	Yes	No	Unknown
<b>Acceptable Use Management</b>			
The acceptable use of all educational equipment and services is defined carefully for all technology participants.	Yes	No	Unknown
All technology participants exhibit an understanding of the required policies and procedures for the use of educational technology.	Yes	No	Unknown
External groups such as parents, school boards, and other influential local organizations are clearly aware of the acceptable use of educational equipment and services, and support the organization in its implementation.	Yes	No	Unknown
The appropriate use of technology in meeting the goals of the organization is clearly defined and applied by all decision makers.	Yes	No	Unknown

## Current Educational Security Practices Survey Worksheet (continued)

### Current Educational Security Practices Survey (cont.)

Practice	Is this practice used by your organization?		
<b>Acceptable Use Management (continued)</b>			
Penalties for inappropriate use are clearly defined and understood by all technology participants.	Yes	No	Unknown
The use and responsibilities for participants in special programs with technology components have been clearly defined and communicated to all participants.	Yes	No	Unknown
Acceptable use includes the communication of the risks of technology use to participants. Acceptable Use Policies have been appropriately defined and communicated to all participants (teachers, students, parents).	Yes	No	Unknown
A process monitoring acceptable use has been defined and implemented. That includes a means for participants to report problems and threats conveyed through the technology.	Yes	No	Unknown
Licensing restrictions and other limitations for the use of technology are communicated clearly to all participants.	Yes	No	Unknown
Mechanisms have been established to identify an unacceptable use and link it to the appropriate individual for evaluation and application of penalties.	Yes	No	Unknown

## Appendix G

### Security Practices Summary

Based on responses to the surveys, summarize the results in the following tables:

#### Summary of General Security Practices

Practice Area	Status		
Security Awareness and Training	Fine	Needs Improvement	Needs Research
Security Strategy	Fine	Needs Improvement	Needs Research
Security Management	Fine	Needs Improvement	Needs Research
Security Policies and Regulations	Fine	Needs Improvement	Needs Research
Collaborative Security Management	Fine	Needs Improvement	Needs Research
Contingency Planning/Disaster Recovery	Fine	Needs Improvement	Needs Research
Physical Security Plans and Procedures	Fine	Needs Improvement	Needs Research
Physical Access Control	Fine	Needs Improvement	Needs Research
System and Network Management	Fine	Needs Improvement	Needs Research
Authentication and Authorization	Fine	Needs Improvement	Needs Research
Incident Management	Fine	Needs Improvement	Needs Research
General Staff Practices	Fine	Needs Improvement	Needs Research

#### Summary of Educational Security Practices

Practice Area	Status		
Content Blocking	Fine	Needs Improvement	Needs Research
Structured Access Management	Fine	Needs Improvement	Needs Research
Regulatory Compliance - COPPA	Fine	Needs Improvement	Needs Research
Regulatory Compliance – Copyright and Licensing Laws	Fine	Needs Improvement	Needs Research
Regulatory Compliance – Federal and State Reporting	Fine	Needs Improvement	Needs Research
Regulatory Compliance – Protection Against Criminal Use of Technology	Fine	Needs Improvement	Needs Research
Acceptable Use Management	Fine	Needs Improvement	Needs Research

## Security Practices Summary (continued)

**Summary of Information Technology (IT) Security Practices**

<b>Practice Area</b>	<b>Status</b>		
Security Awareness and Training	Fine	Needs Improvement	Needs Research
Security Management	Fine	Needs Improvement	Needs Research
Security Policies and Regulations	Fine	Needs Improvement	Needs Research
Monitoring and Auditing Physical Security	Fine	Needs Improvement	Needs Research
System and Network Management	Fine	Needs Improvement	Needs Research
System Administration Tools	Fine	Needs Improvement	Needs Research
Monitoring and Auditing IT Security	Fine	Needs Improvement	Needs Research
Authentication and Authorization	Fine	Needs Improvement	Needs Research
Security Architecture and Design	Fine	Needs Improvement	Needs Research
Vulnerability Management	Fine	Needs Improvement	Needs Research
Encryption	Fine	Needs Improvement	Needs Research

## Appendix H

### Protection Strategy for Educational Practices Worksheet

#### Protection Strategy for Educational Practices Content Blocking (ED1)

#### Questions to Consider

- What training and education initiatives could help your organization maintain or improve its content-blocking practices?
- What funding level is appropriate to support your content-blocking needs?
- Are your policies and procedures sufficient for your content-blocking needs? How could they be improved?
- Who has responsibility for defining and implementing the details of content-blocking? Should anyone else be involved?
- How are problems identified and addressed? Would adjustments in these procedures improve the value of content-blocking?
- What external experts could help you with defining and implementing content-blocking? How will you communicate your requirements? How will you verify that your requirements were met?

#### Strategies

**Issues:** What issues related to content-blocking cannot be addressed by your organization?

## Protection Strategy for Educational Practices Worksheet (continued)

Protection Strategy for Educational Practices Structured Access Management (ED2)	
Questions to Consider	Strategies
<ul style="list-style-type: none"> <li>• What training and education initiatives could help your organization maintain or improve its technology selection and distribution practices?</li> <li>• What funding level is appropriate to support your technology infrastructure needs?</li> <li>• Are your policies and procedures sufficient for your technology access and availability needs? How could they be improved?</li> <li>• Who has responsibility for defining and implementing the decisions on availability, distribution, and access control? Should anyone else be involved?</li> <li>• How are problems identified and addressed? Would adjustments in these procedures improve the value of technology?</li> <li>• What external experts could help you with defining and implementing appropriate levels of availability and access? How will you communicate your requirements? How will you verify that your requirements were met?</li> </ul>	
<p><b>Issues:</b> What issues related to structured access management cannot be addressed by your organization?</p>	

## Protection Strategy for Educational Practices Worksheet (continued)

Protection Strategy for Educational Practices Regulatory Compliance (ED3)	
Questions to Consider	Strategies
<ul style="list-style-type: none"> <li>• What training and education initiatives could help your organization maintain or improve its regulatory compliance practices?</li> <li>• What funding level is appropriate to support your regulatory compliance needs?</li> <li>• Are your policies and procedures sufficient for your regulatory compliance needs? How could they be improved?</li> <li>• Who has responsibility for defining and implementing the details of regulatory compliance? Should anyone else be involved?</li> <li>• How are problems identified and addressed? Would adjustments in these procedures improve the level of regulatory compliance?</li> <li>• What external experts could help you with defining and implementing levels of regulatory compliance? How will you communicate your requirements? How will you verify that your requirements were met?</li> </ul>	
<p><b>Issues:</b> What issues related to regulatory compliance cannot be addressed by your organization?</p>	

## Protection Strategy for Educational Practices Worksheet (continued)

### Protection Strategy for Educational Practices Acceptable Use (ED4)

#### Questions to Consider

- What training and education initiatives could help your organization maintain or improve its acceptable use practices?
- What funding level is appropriate to support your establishing and monitoring acceptable use?
- Are your policies and procedures sufficient for your acceptable use requirements? How could they be improved?
- Who has responsibility for defining and implementing the details of acceptable use? Should anyone else be involved?
- How are problems identified and addressed? Would adjustments in these procedures improve the compliance of acceptable use?
- What external experts could help you with defining and implementing appropriate levels of acceptable use? How will you communicate your requirements? How will you verify that your requirements were met?

#### Strategies

**Issues:** What issues related to acceptable use cannot be addressed by your organization?

## Appendix I

### OCTAVE Criteria Principles to K-12 Risk Methodology

Principle	Applied	When	Applied to Methodology Guidance	Applied at Pilot Site
Self-direction	Yes	Unchanged	Requirement for selection of pilot site	The site managed all of their analysis and planning steps with training guidance from this researcher.
Adaptable measures	Yes	Tailoring	Evaluation criteria adjusted to fit K-12 schools and catalog of practices expanded to include educational issues; other measurements like vulnerability catalog were unchanged from OCTAVE Methodology.	The site applied the practices from the tailored K-12 Catalog of Practices to their planning and decision making. The site selected ITS own unique evaluation criteria for valuing threats.
Defined process	Yes	Tailoring	Detailed guidance, adjusted for changes to Phase 1 and 3, is carried from OCTAVE Methodology.	The site followed much of the sequential process defined in the guidance.
Foundation for continuous change	Yes	Tailoring	Guidance instructing analysis team to consider establishing a foundation for continuous change is carried from the OCTAVE Methodology.	The site discussed monitoring the implementation of its plans and review of the assessment results annually to confirm continued validity. Also follow-on assessments with additional assets to refine the organizational threat perspective were identified.
Forward-looking view	Yes	Tailoring	Guidance instructing analysis team to focus beyond the current issues to consider future requirements is carried from the OCTAVE Methodology.	Security requirements and planning incorporated changes expected in funding, responsibilities, and connectivity proposed for coming school years.
Critical few	Yes	Unchanged	Focus on subset of assets, mapping threats to a range, and prioritization of threats carried over from OCTAVE Methodology.	A subset of assets was selected to identify threats. A subset of potential practices was selected to focus limited resources and address the greatest threats.

## OCTAVE Criteria Principles to K-12 Risk Methodology (continued)

<b>Principle</b>	<b>Applied</b>	<b>When</b>	<b>Applied to Methodology Guidance</b>	<b>Applied at Pilot Site</b>
Integrated management	Yes	Tailoring	Phase 3 continues to include strategic and organizational perspectives that were expanded to include the educational perspective.	Both strategic and organizational issues were included in planning. Educational issues were not viewed as potential threat areas for the pilot site.
Open communication	Yes	Unchanged	Workshop format carried over from OCTAVE Methodology.	Dialogue about security issues among participants in the analysis team was identified as a key result in the pilot survey responses.
Global perspective	Yes	Tailoring	Summarization process for survey results added to provide a consensus process for current practices. Other workshops carried over from OCTAVE Methodology.	Members of the analysis team provided a range of expertise that spanned beyond the technical aspects of security into the educational curriculum and administrative management.
Teamwork	Yes	Unchanged	Requirements for pilot site	The work was addressed by an analysis team of five individuals, and each contributed to the success of the result.

## Appendix J

## OCTAVE Criteria Attributes to K-12 Risk Methodology

Attribute	Applied	When	Applied to Methodology Guidance	Applied at Pilot Site
Analysis team	Yes	Unchanged	Requirement for site selection	Team of five individuals agreed to perform the assessment.
Augmenting analysis team skills	Yes	Unchanged	Consideration for completeness of analysis team at pilot site and considered for Phase-2 decision	Consideration was given to augmenting the team with technical expertise for Phase 2 but was determined to not be an appropriate choice at this time.
Catalog of practices	Yes	Tailoring	OCTAVE Catalog of Practices expanded to incorporate educational issues	The expanded catalog of practices through the survey and protection strategy worksheets was incorporated into the methodology and applied.
Generic threat profile	Yes	Unchanged	OCTAVE Methodology threat profiles carried over to tailored methodology unchanged	Four generic threat profiles were used for threat consideration. They were expanded with two additional threats considered important to the pilot site.
Catalog of vulnerabilities	Yes	Unchanged	OCTAVE Methodology threat profiles carried over to tailored methodology unchanged	Consideration for a catalog of vulnerabilities was provided in Phase 2, but Phase 2 was not performed by the pilot site.
Defined evaluation activities	Yes	Tailoring	Detailed guidance is provided for each activity and includes instructions for all worksheets.	Step-by-step guidance was provided. In some areas, the analysis team chose to vary the sequence based on their organizational issues.
Documented evaluation results	Yes	Tailoring	Worksheets are provided for all steps of the evaluation to provide a location for documenting each step of each activity.	Worksheets were completed, and a summary report of the findings was prepared.

## OCTAVE Criteria Attributes to K-12 Risk Methodology (continued)

Attribute	Applied	When	Applied to Methodology Guidance	Applied at Pilot Site
Evaluation scope	Yes	Unchanged	Activity in the planning session with the pilot site	A specific range of organizational units (those under the responsibility of analysis team members) was selected.
Next Steps	Yes	Tailoring	Phase 3 is a planning process that establishes a protection strategy for the organization to implement.	The pilot site selected three areas of practices to apply and developed a plan for addressing the next steps in the application effort.
Focus on risk	Yes	Tailoring	The evaluation criteria are changed, but use of the evaluation criteria as applied to threats to establish a prioritization based on the impact is carried over unchanged.	The impacts of threats were evaluated based on evaluation criteria important to the organization. Plans were defined in Phase 3 based on the highest risks, which resulted in different selections than those initially identified in the data-gathering steps of Phase 1.
Focused activities	Yes	Tailoring	Activities are formed to maintain the focus of the analysis team on each separate issue (asset identification, security requirements, threat evaluation, impact evaluation, analysis and planning) that builds in a logical sequence to produce the resulting plan.	Each step assembled another layer of information that formed a broad picture of threat and opportunities for protection based on the current environment.
Organizational and technological issues	Yes	Tailoring	Activities are based on the catalog of practices that is expanded to include educational issues in addition to organizational and technological ones.	The application of a broad catalog of practices provided inclusion of both types of issues.
Organizational and information technology participation	Yes	Tailoring	Requirement for the pilot site selection	The analysis team included both organizational and technical participation.
Senior management participation	Yes	Tailoring	The coordinator for the analysis team was responsible for keeping senior management apprised of the status and results	Senior management received interim briefings and will be the recipient of the final output - a security risk management plan.

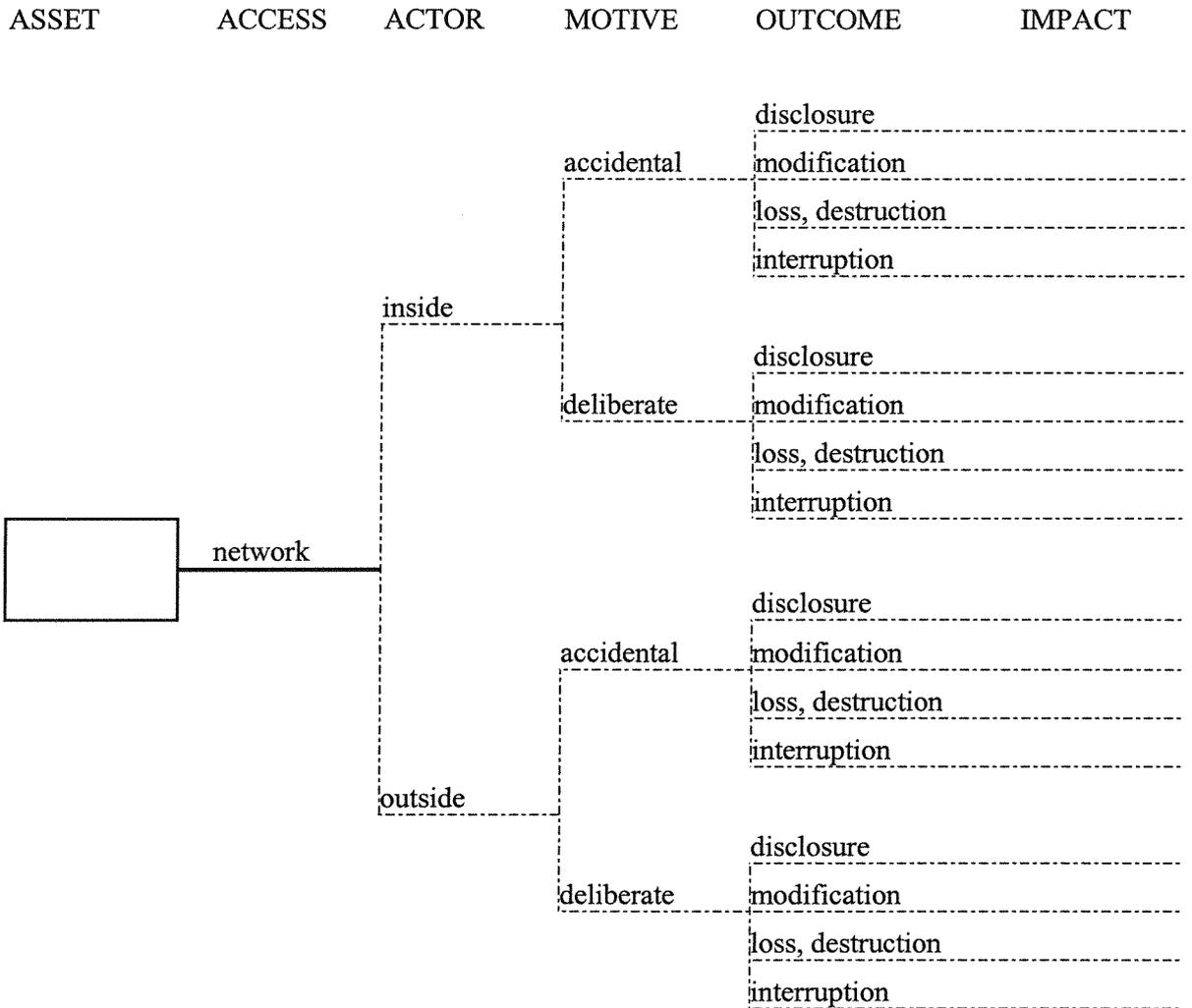
## OCTAVE Criteria Attributes to K-12 Risk Methodology (continued)

Attribute	Applied	When	Applied to Methodology Guidance	Applied at Pilot Site
Collaborative approach	Yes	Unchanged	Selection of the analysis team was based on communication needs with a focus on teamwork.	Analysis team participants had a working relationship that was augmented by the use of the risk assessment methodology.

## Appendix K

### Generic Threat Tree Example

#### Human Actors Using Network Access



## Appendix L

### Pilot Site Survey Responses

JOB TITLE: *Technology Coordinator*

1. How has the use of the methodology expanded your understanding of K-12 school information security issues?

*The methodology was highly effective in increasing my understanding of security issues in three distinct ways. First, having an expert work with us to understand security issues in general provided an important overview of the process and highlighted important areas of concern. Second, having access to tools and strategies (the workbooks) allowed us to understand the specific issues that we had to address. Finally, the methodology provided formal opportunities to discuss our current security practices with my colleagues. Although we have opportunities to work together, we never had a chance to share and discuss our security practices. The methodology provided the opportunity for the administrative, technical, and instructional technology staff to engage in serious discussions about security.*

2. How have plans for actions, mitigations, and protection strategies developed with the methodology addressed the school's security concerns?

*With the installation of a wide area network and the increasing reliance on Web services, I became very concerned about protecting the integrity of our data, as well as the privacy of students and staff. I was also concerned that we did not have important security procedures in place at all levels of the system. The methodology confirmed that we needed to address our security concerns, and allowed our group to come to that conclusion by collaboration and focused discussion.*

*The methodology also provided:*

- 1. Opportunities for our group to have discussions about important security issues*
- 2. A framework and context for the discussions*
- 3. A sense of commitment from all parties to develop an action plan and to make security a district priority.*

## Pilot Site Survey Responses (continued)

JOB TITLE: *Technology Coordinator (continued)*

3. How has use of the methodology better prepared you to address information technology (IT) decisions and security issues in the future?

*The methodology established a process for discussions and security reviews that our team will continue to use. It also emphasized the importance of continued security awareness and increased our commitment to making sure that we have appropriate security measures in place.*

4. Other comments or suggestions?

*The security methodology allowed us to engage in our own problem-solving strategies by reflecting on our current practices and engaging in dialogue about possible solutions. It was effective because we took ownership over our problems rather than having an outside consultant provide us with solutions. The methodology effectively guided our discussions and helped us to understand the threats to our security. The emphasis on a collaborative exploratory process allowed us to begin to make meaningful changes in our security practices and commit to ongoing review and improvement.*

JOB TITLE: *Technical Supervisor*

1. How has the use of the methodology expanded your understanding of K-12 school information security issues?

*It has given us a template to refer to so that we can organize our security objectives, risks, and policies.*

2. How have plans for actions, mitigations, and protection strategies developed with the methodology addressed the school's security concerns?

*The methodology addressed all of our security concerns and in fact enlightened us to several security issues that we would not have addressed without the methodology.*

## Pilot Site Survey Responses (continued)

JOB TITLE: *Technology Supervisor (continued)*

3. How has use of the methodology better prepared you to address information technology (IT) decisions and security issues in the future?

*The methodology has prepared us to address future security decisions by enabling us to focus on the weak areas in our security. Without the methodology, too much time may have been spent on redundant tasks. The methodology will enable us to approach future security issues in an organized manner.*

4. Other comments or suggestions?

*The methodology that you present has given us the foundation to build good IT security policies.*

*Thank you.*

JOB TITLE: Network Specialist

1. How has the use of the methodology expanded your understanding of K-12 school information security issues?

*The methodology increased the awareness of the participants about certain areas of security that were not previously addressed.*

2. How have plans for actions, mitigations, and protection strategies developed with the methodology addressed the school's security concerns?

*The plans developed by the methodology have included certain aspects of security that need to be reviewed and developed.*

## Pilot Site Survey Responses (continued)

JOB TITLE: *Network Specialist (continued)*

3. How has use of the methodology better prepared you to address information technology (IT) decisions and security issues in the future?

*The methodology focused the group to formulate a plan of action to rectify outstanding security issues.*

4. Other comments or suggestions?

*Continue development of additional descriptions and additional instructions to alleviate confusion.*

*Include examples and case studies. A Web site with forms and sample tools would be helpful.*

*Recommendations for the scope of participants may help other school districts. A timeline to follow to complete the methodology would help.*

JOB TITLE: *Administrative Manager*

1. How has the use of the methodology expanded your understanding of K-12 school information security issues?

*This methodology really gives me an approach to begin seriously thinking security technology. The approach is more of a template to jump start us and get us to focus on the issue. Considering all of us who participate in the program, we would never, or it might be virtually impossible, find the time to talk about preventive security. Furthermore, the methodology helps me to focus on specific issues such as: student records, the human factor, and definitely physical security.*

2. How have plans for actions, mitigations, and protection strategies developed with the methodology addressed the school's security concerns?

*The methodology helps me to look at our security in stages instead of just finding solutions to problem; for example, critical asset, user community, and system problems. It also helped me to examine our security practices which in most cases I would never find the time to even address.*

## Pilot Site Survey Responses (continued)

JOB TITLE: *Administrative Manager (continued)*

3. How has use of the methodology better prepared you to address information technology (IT) decisions and security issues in the future?

*The key here is that the methodology will help me to prepare or develop long- and short-range plans to upgrade my security-related services.*

*This will include us establishing clear policies and procedures for my user community.*

*Enforce password policies and find a way for us to better keep track of people (users) entering and exit our system.*

4. Other comments or suggestions?

*The session meetings as a group gave me a new approach of evaluating and looking at information, technology security, staff, and physical security.*

JOB TITLE: *Asst. Computer System Manager*

1. How has the use of the methodology expanded your understanding of K-12 school information security issues?

*The methodology allowed me to organize my concerns and ideas about security issues and risks. It helped me focus on the essential risks and gave me a way to define procedures for a solution to the issues.*

2. How have plans for actions, mitigations, and protection strategies developed with the methodology addressed the school's security concerns?

*The plans developed using the methodology gave me something concrete to work with.*

## Pilot Site Survey Responses (continued)

JOB TITLE: *Asst. Computer System Manager(continued)*

3. How has use of the methodology better prepared you to address information technology (IT) decisions and security issues in the future?

*The methodology has given me a framework to address security issues; a way of taking large amorphous issues and translating them into smaller more manageable pieces that can be solved in a more effective manner.*

4. Other comments or suggestions?

*Because of the limited time and personnel in a school environment, some of the format should be collapsed a bit.*

## Appendix M

### Abbreviations

ABA – American Bankers Association

ACLU – American Civil Liberties Union

AICPA – American Institute of Certified Public Accountants

ALA – American Library Association

AOL – America Online

ASL – American Student List

AUP – acceptable use policy

BGP – border gate protocol

BSI – British Standards Institute

CERT/CC – Computer Emergency Response Team Coordination  
Center

CDA – Communications Decency Act of 1996

CFAA – Computer Fraud and Abuse Act

CIPA – Children’s Internet Protection Act of 2000

CIPB – Critical Infrastructure Protection Board

CIS – Computer Intrusion Squad

COBIT – Control Objects for Information Technology

COPA – Child Online Protection Act of 1999

COPPA – Children’s Online Privacy Protection Act

CoSN – Consortium for School Networking

CSI – Computer Security Institute

## Abbreviations (continued)

CVE – Common Vulnerabilities and Exposures

DHHS – U.S. Department of Health and Human Services

DHS/IAIP – U.S. Department of Homeland Security Infrastructure  
Analysis Infrastructure Protection

DMCA – Digital Millennium Copyright Act of 1998

ECPA – Electronic Communications Privacy Act

ED – U.S. Department of Education

EFL – Exploring the Future of Learning

EPIC – Electronic Privacy Information Center

ESEA – Elementary and Secondary Education Act of 1965

FBI – Federal Bureau of Investigation

FCC – Federal Communications Commission

FERPA – Family Educational Rights and Privacy Act

FOIA – Freedom of Information Act

FRAP – Facilitated Risk Analysis Process

FTC – Federal Trade Commission

GIAC – General Information Assurance Certification

GISRA – Government Information Security Reform Act

GLBA – Gramm-Leach-Bliley Act of 1999

GSEC – GIAC Security Essentials

HIPAA – Health Insurance Portability Accountability Act of 1996

I3P – Institute for Information Infrastructure Protection

## Abbreviations (continued)

ICCS™ – iWatchdog™ Commercial Certification Service

ICRA – Internet Content Rating Association

IPAK – Information Protection Assessment Kit by the CSI

ISACA – Information Systems Audit and Control Association

ISO – International Standards Organization

ISP – Internet Service Provider

ISTE – International Society for Technology in Education

IT – Information Technology

LAN – local area network

MPEG – Moving Picture Experts Group

NCAC – National Coalition Against Censorship

NCLB – No Child Left Behind Act

NCREL- North Central Regional Educational Laboratory

NETS-A – National Education Technology Standards for School

Administrators

NETS-S – National Education Technology Standards for School

Students

NETS-T – National Education Technology Standards for School

Teachers

NIST – National Institute of Standards and Technology

NRCCUA – National Research Center for College and University

Admissions

## Abbreviations (continued)

NSBA – National School Boards Association

NSBF – National School Boards Foundation

OCTAVE – Operationally Critical Threat, Asset, and Vulnerability  
Evaluation

PICS – Platform for Internet Content Selection

PPRA – Protection of Pupil Rights Amendment

PTA – Parent Teacher’s Association

RIAA – Recording Industry Association of America

SANS – System Administration, Audit, Network, Security Institute

SEI – Carnegie Mellon Software Engineering Institute

SFG – Security Focus Group of the CoSN

SLD – School and Libraries Division

SPSD – Scarsdale Public School District

TEACH – Technology Education and Copyright Harmonization Act  
of 2001

TSI – Technology Support Index

TSSA – Consortium for Technology Standards for School  
Administrators

UFCWS – United Federation of Child Safe Web Sites

U.S. – United States

USAC – Universal Service Administration Company

## Abbreviations (continued)

USA PATRIOT – Uniting and Strengthening America by Providing  
Appropriate Tools Required to Intercept and Obstruct  
Terrorism

UT – University of Texas

W3C – World Wide Web Consortium

WAN – wide-area network

WBEC – Web-Based Education Commission

## Reference List

- ALA. (1999). The Top Ten Reasons Why the Internet Still Will Not Replace the Public Library. *One Librarian, American Librarian Association*. Retrieved December 3, 2001, from the World Wide Web: <http://www.geocities.com/SoHo/Nook/8823/stillhere.html>.
- Alberts, C., Behrens, S., Pethia, R., & Wilson, W. (2000). *Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE®) Framework, Version 1* (CMU/SEI-99-TR-017). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University.
- Alberts, C., & Dorofee, A. (2001a). *OCTAVE® Criteria, Version 2.0*. Pittsburgh PA: Software Engineering Institute, Carnegie Mellon University.
- Alberts, C., & Dorofee, A. (2001b). *OCTAVE® Threat Profiles*. Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University.
- Alberts, C., & Dorofee, A. (2001c). *Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE®) Method Implementation Guide Version 2.0*. Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University.
- Alberts, C., & Dorofee, A. (2002). *Managing Information Security Risks: The OCTAVE® Approach*. Addison Wesley.
- Alberts, C., Dorofee, A., & Allen, J. (2001). *OCTAVE® Catalog of Practices, Version 2.0*. Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University.
- Allen, J. (2001). *The CERT® Guide to System and Network Security Practices*. Upper Saddle River, NJ. Addison-Wesley.
- Allen, J., Alberts, C., Behrens, S., Laswell, B., & Wilson, W. (2000). Improving the Security of Networked Systems. *CrossTalk*, Retrieved July 25, 2002, from the World Wide Web: <http://www.stsc.hill.af.mil/crosstalk/2000/oct/allen.asp>.
- Allen, J., & Sledge, C. (2002). Information Survivability: Required Shifts in Perspective. *CrossTalk, The Journal of Defense Software Engineering*, 15, 7-9.
- Anthony, B., & Cohn, T. (2000). Putting Parents Back in Charge of Kids' Privacy. *Computerworld*, May 15, 2000, 36.
- Armstrong, A., & Casement, C. (2000). *The Child and the Machine How Computers put our Children's Education at Risk*. Beltsville, MD: Robins Lane Press.

- Armstrong, S., Sibley, R., & Samara, P.. (2003). Privacy, Security, and Identity in a Networked, Data Driven Education Environment. *Exploring the Future of Learning*. Retrieved September 8, 2003, from the World Wide Web: <http://www.futureoflearning.org>.
- AWS. (2002). *OnTarget*. AWS Convergence Technologies, Inc . Retrieved May 20, 2003, from the World Wide Web: <http://www.ontargetus.com>.
- Azizuki, D. (2003). High School Suspends Student Hackers Who Changed Grades. *The Mercury News*. Retrieved March 12, 2003, from the World Wide Web: [http://www.siliconvalley.com/mld/siliconvalleyss/special\\_package/security/5334721.htm](http://www.siliconvalley.com/mld/siliconvalleyss/special_package/security/5334721.htm).
- Balkin, J., Noveck, B., & Roosevelt, K. (1999). Filtering the Internet: A Best Practices Model. *Information Society Project, Yale Law School*. Retrieved July 22, 2002, from the World Wide Web: <http://islandia.law.yale.edu/isp/papers/Filters0208.pdf>.
- Bell, S. (2001). Web-Based Utilities for Learning and Collaboration in the Classroom. *Syllabus, July*, 32-35.
- Biersdorfer, J. D. (1999). Typing for the Show-and-Tell Set: How Early is too Early. *The New York Times*, pp. G11.
- Biskupic, J. (1999). In Shaping of Internet Law, First Amendment is Winning. *The Washington Post*, pp. A2.
- Blackwell, J. (2002). Library Hacker Gets Jail Time. *Democrat and Chronicle*. Retrieved August 21, 2002, from the World Wide Web: [http://www.democratandchronicle.com/news/0815story110800\\_news.shtm](http://www.democratandchronicle.com/news/0815story110800_news.shtm).
- Bradsher, K. (2000). Town Rejects Bid to Curb Library's Internet Access. *New York Times*, pp. A12.
- Brewin, B. (2001). Massive ASP Deal 'Unprecedented'. *Computerworld*, 35(35), 1,16.
- Brooke, J. (2001). Delegates in Japan Debate Problem of Commercial Exploitation. *New York Times*, pp. A12.
- Bruckman, A. (2002). The Future of E-Learning Communities. *Communications of the ACM*, 45, 60-63.
- Brulliard, K. (2003). Student Charged With Hacking at U-Texas. *The Washington Post*. Retrieved March 19, 2003, from the World Wide Web: <http://www.washingtonpost.com/wp-dyn/articles/A27370-2003Mar14.html>.

- Brykczynski, B., & Small, B. (2003). Securing Your Organization's Information Assets. *CrossTalk, The Journal of Defense Software Engineering*, 16(5).
- BSI. (1995). *Information Security Management, Part 1: Code of Practice for Information Security Management and Systems*. British Standards Institution, BS7799.
- Cannon, R. (2001). Complying with COPPA: Children's Privacy in an Online Jungle. *Webtechniques*, 6(8), 34-38.
- Carpenter, J. (2001). Computer Security Issues that Affect Federal, State, and Local Government. *House of Representatives Committee on Government Reform, Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations*. Retrieved August 30, 2001, from the World Wide Web:  
[http://www.cert.org/congressional\\_testimony/Carpenter\\_testimony\\_Aug2029.html](http://www.cert.org/congressional_testimony/Carpenter_testimony_Aug2029.html)  
 1.
- Carr, J. (2001). Biometric Devices: the Next Wave. *Network Magazine*, October 2001, 48-50,52.
- Cattagni, A., & Westat, E. F. (2001). *Internet Access in U.S. Public Schools and Classrooms: 1994-2000 (Statistics in Brief NCES 2001-071)*. National Center for Education Statistics. U.S. Department of Education.
- CERT. (1998). *Security of the Internet*. Retrieved August 15, 2002, from the World Wide Web: [http://www.cert.org/encyc\\_article/tocencyc.html](http://www.cert.org/encyc_article/tocencyc.html).
- CERT. (2003a). *CERT/CC Statistics 1988-2003*. Retrieved May 20, 2003, from the World Wide Web: [http://www.cert.org/stats/cert\\_stats.html](http://www.cert.org/stats/cert_stats.html).
- CERT. (2003b). *CERT/CC Overview Incident and Vulnerability Trends*. Retrieved May 20, 2003, from the World Wide Web: <http://www.cert.org/present/cert-overview-trends/module-2.pdf>.
- Chamberlin, W. S. (2001). Face-to-Face vs. Cyberspace Finding the Middle Ground. *Syllabus*, 15(5), 10-11, 32.
- Chambers, J., Lieberman, J., Parrish, T., Kaleba, D., Campen, J. V., & Stullich, S. (2000). *Study of Education Resources and Federal Funding: Final Report (Executive Summary)*. Planning and Evaluation Service, U.S. Department of Education Office of the Under Secretary.
- Chapin, R. (1999). Content Management, Filtering and the World Wide Web. *The Journal (Technological Horizons In Education)*, 27(2), 44.

- CIPB. (2003). The National Strategy to Secure Cyberspace. *The President's Critical Infrastructure Protection Board*. Retrieved February 17, 2003, from the World Wide Web: [http://www.whitehouse.gov/pcipb/cyberspace\\_strategy.pdf](http://www.whitehouse.gov/pcipb/cyberspace_strategy.pdf).
- Clark, E. (2001). Oregon School District Provides Higher (Bandwidth) Learning. *Network Magazine*, 16(12), 64-69.
- Clayton, M., & Watkins, A. (2002). Assessment and Integrity in the Digital Arts. *Syllabus*, 15, 31-34.
- Cohen, A. (2000). No Web for You. *Fortune Small Business*, 7, 44-56.
- Colkin, E. (2001). Kids These Days. *Informationweek*, February 12, 2001, RB1-RB8.
- Colkin, E. (2002). Whose Rules. *Informationweek*, March 11, 2002, 30-37.
- Cope, J., & Brewin, B. (2000). Students Unplugged but Well Connected. *Computerworld*, September 11, 2000, Retrieved May 21, 2001, from the World Wide Web: [http://www.computerworld.com/cwi/story/2000,1199,NAV2047\\_STO49911,49900.html](http://www.computerworld.com/cwi/story/2000,1199,NAV2047_STO49911,49900.html).
- CoSN. (2002). *Safeguarding the Wired Schoolhouse*. Washington, DC: Consortium for School Networking. Retrieved from the World Wide Web September 12, 2002: <http://www.safewiredschools.org>.
- Cuban, L. (2001). *Oversold & Underused Computers in the Classroom*. Cambridge, MA: Harvard University Press.
- Cunningham, C. (2000). Rights of Way: Adaptive Technologies on Campus. *Syllabus*, 14(2), 32,34,36.
- Davis, J. (2000). Class Acts. *The Industry Standard Grok*, October 2000, 26-36.
- DHHS. (2003). *RIN 0938-AI57 Health Insurance Reform: Security Standards*. Washington DC: US Department of Health and Human Services.
- Dickerson, L. A. (2002). *Homeless Children Need not be School-less Children*. Pittsburgh: La Roche College Center for the Study of Ethics.
- ED. (1997). *Emerging Priorities*. Retrieved March 22, 2002, from the World Wide Web: <http://www.air.org/forum/Issues.htm>.
- ED. (2000a). *e-Learning Putting a World-Class Education at the Fingertips of all Children*. Congressional Report. Washington DC: U.S. Department of Education.

- ED. (2000b). *E-Rate and the Digital Divide: a Preliminary Analysis From the Integrated Studies of Educational Technology*. US Department of Education - Office of the Under Secretary 00-17. Washington, DC: The Urban Institute.
- ED. (2001). *The No Child Left Behind Act of 2001 Executive Summary*, U.S. Department of Education. Washington, DC. Retrieved March 3, 2003, from the World Wide Web: <http://www.ed.gov/offices/OESE/esa/exec-summ.html>.
- ED (2002a). *Family Educational Rights and Privacy Act (FERPA)*. Retrieved February 18, 2003, from the World Wide Web: <http://www.ed.gov/offices/OM/fpco/ferpa/index/html>.
- ED (2002b). *Protection of Pupil Rights Amendment (PPRA)*. Retrieved February 18, 2003, from the World Wide Web: <http://www.ed.gov/offices/OM/fpcoppra/index.html>.
- ED (2002c). *No Child Left Behind - A Desktop Reference*. Office of the Under Secretary. Retrieved March 1, 2003, from the World Wide Web: <http://www.ed.gov/offices.oese/reference.pdf>.
- EDUCAUSE. (2002). *Higher Education Contribution to National Strategy to Secure Cyberspace*. Retrieved February 16, 2003, from the World Wide Web: <http://www.educause.edu/cr/library/pdf/net00027.pdf>.
- EFF. (2002). EFF Analysis of the Provisions of the USA PATRIOT Act. *Electronic Frontier Foundation*. Retrieved April 3, 2002, from the World Wide Web: [http://www.eff.org/Privacy/Surveillance/Terrorism\\_militias](http://www.eff.org/Privacy/Surveillance/Terrorism_militias).
- Ehrmann, S. (2000). The Flashlight Program Evaluating Instructional Uses of the Web. *Syllabus*, 14(2), 38,40,42.
- Eisler, D. (2000). The Portal's Progress a Gateway for Access, Information, and Learning Communities. *Syllabus*, 14(2), 12-14,16,18.
- Enderle, J., (2003), Are School Networks as Safe as We Think?, *School Planning & Management*, 42(4), 38-41.
- EPIC. (1999a). Faulty Filters: How Content Filters Block Access to Kid-Friendly Information on the Internet. In EPIC (Ed.), *Filters & freedom Free Speech Perspectives on Internet Content controls* (pp. 53-66). Washington DC: Electronic Privacy Information Center.
- EPIC (Ed.). (1999b). *Filters & Freedom Free Speech Perspectives on Internet Content Controls* (First ed.). Washington, DC: Electronic Privacy Information Center.

- EPIC (2002). *Opinion of the Court, May 31, 2002*. Retrieved May 20, 2003, from the World Wide Web: [http://www.epic.org/free\\_speech/cipa/opinion\\_e.d.pa.html](http://www.epic.org/free_speech/cipa/opinion_e.d.pa.html).
- EPIC. (2003). Privacy and Consumer Profiling. *Electronic Privacy Information Center*. Retrieved March 31, 2003, from the World Wide Web: <http://www.epic.org/privacy/profiling>.
- FBI. (1998). *A Parent's Guide to Internet Safety*. Washington, DC: U.S. Department of Justice.
- Fienberg, H. (2001). Censorware Can't Replace Parents. *liberzine.com*, Retrieved January 14, 2002, from the World Wide Web: <http://www.liberzine.com/howardfienberg/010415censorware.htm>.
- Finkelstein, S. (2001). *Information About Labeling and Rating Systems*. Retrieved December 3, 2001, from the World Wide Web: <http://www.mit.edu/activities/safe/laeling/summary.html>.
- Fisher, S. (2000). *Medium, Method, and Message: Why We Can Measure the Pedagogic Effectiveness of Instructional Technology*. Paper presented at the Computing and Philosophy (CAP) Conference 2000.
- FTC. (2003). KidzPrivacy. Federal Trade Commission. Retrieved May 20, 2003, from the World Wide Web: <http://www.ftc.gov/bcp/online/kidzprivacy/index.html>.
- GAO. (1998). *Internet filtering Systems: Report of the Committee on Commerce, Science, & Transportation*. Washington, DC: United States Congress, US GPO.
- GAO. (2001). *Characteristics and Choices of Internet Users (GAO-01-345)*. Washington, DC: U.S. General Accounting Office: Report to the Ranking Minority Member, Subcommittee on Telecommunications, Committee on Energy and Commerce, House of Representatives.
- Gaunt, M. (2002). A Bridge to the Future. *Syllabus*, 15(8), 12-16.
- Golden, D. (2000). Is ZapMe Collecting Data on School Kids? *Wall Street Journal Online*, January 16, 2000. Retrieved February 16, 2003, from the World Wide Web: <http://zdnet.com.com/2100-11-517919.html>.
- Hanson, W. (2001). Student-Centered Education. *Government Technology*, January 2001, 14-16.
- Harrison, A. (2000). Symantic: List of Blocked Sites Breaks Copyright Laws. *Computerworld*, March 20, 2000, Retrieved May 21, 2001, from the World Wide Web:

[http://www.computerworld.com/cwi/story/2000,1199,NAV2047\\_STO41897,41800.html](http://www.computerworld.com/cwi/story/2000,1199,NAV2047_STO41897,41800.html).

- Healy, J. (1998). *Failure to Connect How Computers Affect Our Children's Minds - and What We Can Do About It*. New York: Simon & Schuster.
- Heins, M. & Cho, C. (2001) Internet Filters a Public Policy Report, *National Coalition Against Censorship*. Retrieved July 31, 2002, from the World Wide Web: <http://www.ncac.org/issues/internetfilters.html>.
- Holmes, W. N. (1999). The Myth of the Educational Computer. *Computer*, 32(9), 36-42.
- Hunter, C. D. (1999). *Internet Filtering Effectiveness: Testing Over and Under-inclusive Blocking Decisions of Four Popular Filters*. University of Pennsylvania, Philadelphia.
- I3P. (2003). Cyber Security Research and Development Agenda. *Institute for Information Infrastructure Protection*. Retrieved February 1, 2003, from the World Wide Web: <http://www.thei3p.org/documents/2003-Cyber-Security-RD-Agenda.pdf>.
- ISTE. (2002). National Education Technology Standards for Administrators. *International Society for Technology in Education*. Retrieved July 31, 2002, from the World Wide Web: <http://www.iste.org>.
- Johnston, G. (2002). Record Labels Sue IPSs Over Access to Site. *Computerworld*. Retrieved August 20, 2002, from the World Wide Web: <http://computerworld.com/governmenttopics/legalissues/story/0,10801,73612,00.htm>.
- Kallick, B., & Wilson, J. (Eds.). (2001). *Information Technology for Schools*. San Francisco: Jossey-Bass.
- Kavanaugh-Brown, J. (2000). Rising to the Urban Challenge. *Government Technology*, June 2000, 56-57.
- Kenneally, E. (2002). Who's Liable for Insecure Networks. *Computer*, 35(6), 93-95.
- King, C. (2001). Filtering Software Is Not Up to Snuff. *Internetnews.com*, Retrieved January 14, 2002, from the World Wide Web: [http://www.internetnews.com/business/article/2000,,2009\\_59016,59000.html](http://www.internetnews.com/business/article/2000,,2009_59016,59000.html).
- Klosek, J. (2000). Court Strikes Down Content Law, but Play it Safe when Targeting Children. *Mass High Tech*, July 24-30 2000, 34.
- Kovacich, G. (1998). *Information Systems Security Officer's Guide*: Butterworth-Heinemann.

- Kranich, N. (2001). Why Filters Won't Protect Our Children: Libraries, Democracy and Access. *iMC, June 22, 2001*, Retrieved September 5, 2001, from the World Wide Web: [http://www.cisp.org/imp/june\\_2001/2006\\_2001kranich.htm](http://www.cisp.org/imp/june_2001/2006_2001kranich.htm).
- Kuznia, R. (2003). Newark Hacker May be Expelled. *The Argus*. Retrieved June 18, 2003, from the World Wide Web: <http://www.theargusonline.com/Stories/0,1413~1971~1448608,00.html>
- Landers, J. (2002). As Threat of Cyber Attacks Grows, Security Specialist Blame Faulty Software. *Newsfactor Network*. Retrieved August 23, 2002, from the World Wide Web: <http://www.newsfactor.com/perl/story/19104.html>.
- Lane III, F. S. (2000). *Obscene Profits*. New York: Routledge.
- Lange, S., Davis, J., Jaye, D., Erwin, D., Mullarney, J., Clarke, L., & Loesch, M. (2000). *e-risk Liabilities in a Wired World*. Cincinnati OH: National Underwriter Co.
- Lanz, J. (2002). Prioritizing Aspects of Technology Risk Assessment and Mitigation. *Banking Accounting & Finance, December, 2002*. 19-26.
- LaRue, J. (2000). *Filtering Mechanisms and Issue*. Retrieved January 14, 2002, from the World Wide Web: <http://doublas.lib.co.us/laru/articles/filtering.html>.
- LeBaron, J., & Collier, C. (Eds.). (2001). *Technology in its Place*. San Francisco: Jossey-Bass.
- Legon, J. (2003). Student Hacks School, Kills Class Files. Retrieved June 11, 2003, from the World Wide Web: <http://www.cnn.com/2003/TECH/internet/06/10/school.hacked/index.html>.
- Lesniak, R. (2002). Blended Threats. *Syllabus, 16*, 22-23.
- Levine, R. (2000). Iowa Gives Handheld PCs to Fifth-graders. *Government Computer News/State & Local, August 2000*, 26,28.
- Li, P. (2000). Internet Filtering--The Debate Continues. *InfoTrac Web: Computer Database, 20(9)*, 48.
- Lieber, D., (2004)., Hey! Where's the Problem? *Star-Telegram.com*. Retrieved January 15, 2004, from the World Wide Web:[http://www.dfw.com/mld/dfw/news/columnist/dave\\_lieber/764362.htm](http://www.dfw.com/mld/dfw/news/columnist/dave_lieber/764362.htm).
- Lipson, H. (2002). *Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues*. Pittsburgh: Software Engineering Institute, Carnegie Mellon University.

- Lipson, H., & Fisher, D. (1999). *Survivability - A New Technical and Business Perspective on Security*. Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University.
- Littman, M. K. (1998). Security in the Telelearning Environment. Part II: Cyberproblems and Cyberpolicies. *Hyper Nexus*, 8(2), 11-18.
- Mackenzie, E., & Goldman, K. (2000). *Computer Abuse, Information Technologies and Judicial Affairs*. Paper presented at the SIGUCCS 2000, Richmond, VA.
- Marcroft, T. (1998). Safety First: Managing the Internet in School. *The Journal (Technological Horizons in Education)*, 26(5), 71.
- McKnight, W. (2002). What is Information Assurance? *CrossTalk the Journal of Defense Software Engineering*, 15, 4-6.
- McNabb, M. L., Valdez, G., Nowakowski, J., & Hawkes, M. (1999). *Technology Connections for School Improvement Planners' Handbook*. Planner's Handbook RJ6006301. U.S. Department of Education.
- Metz, R. (2003). Report Accesses Student Info Through District's Open Wireless Network. *The Mercury News*. Retrieved July 1, 2003, from the World Wide Web: <http://www.siliconvalley.com/mld/siliconvalley/6184495.htm>
- Meyer, J. (2000). Power of the People. *American City & County*, 115(15), 20,22,24-25,28,30.
- Moad, J. (2001). Tracking Down the Nasty Guys. *eWeek, December 17/24, 2001*, 40,42.
- Morgan, L. (2000). Blind Faith Doesn't Make for Good Security. *Informationweek: April 17, 2000*, 17.
- NETS. (2002). *National Educational Technology Standards for Teachers - Preparing Teachers to Use Technology*. International Society for Technology in Education.
- Neumann, P. G., & Weinstein, L. (1999). Risks of Content Filtering. *Communications of the ACM*, 42(11), 152.
- Norris, C., Soloway, E., & Sullivan, T. (2002). Examining 25 Years of Technology in U.S. Education. *Communications of the ACM*, 45, 15-18.
- NSBF. (2002a). Are we There Yet? *National School Boards Foundation*. Retrieved July 31, 2002, from the World Wide Web: <http://www.nsb.org/report.htm>.

- NSBF. (2002b). Research and Guidelines for Children's Use of the Internet. *National School Boards Foundation*. Retrieved July 31, 2002, from the World Wide Web: <http://www.nsbf.org/safe-smart/full-report.htm>.
- Null, C. (2003). Google: Net Hacker Tool du Jour. *Wired News*. Retrieved March 12, 2003, from the World Wide Web: <http://www.wired.com/news/infostructure/0.1377.57897.00.html>.
- Oklyzko, A., (2000). Internet Growth: Myth and Reality, Use and Abuse, *Information Impacts Magazine, November 2000*. Retrieved April 14, 2003, from the World Wide Web: [http://www.cisp.org/imp/november\\_2000/odlyzko/11\\_00odlyzko.htm](http://www.cisp.org/imp/november_2000/odlyzko/11_00odlyzko.htm).
- O'Toole, C. (2002). Wired: What Happens When Every Student and Teacher has 24/7 Computer Access? *Pittsburgh, August 2002*, 88-93.
- Parker, D. (1998). *Fighting Computer Crime*. John Wiley & Sons, Inc.
- Patterson, D. (2002). Along the Disability Divide. *Government Technology's Electronic Government*, 3, 8-13.
- Peltier, J. (2003). *How to conduct a Network Vulnerability Assessment*. Retrieved September 28, 2003, from the World Wide Web: <http://www.peltierassociates.com/presentations/csinetsecnva-short.pdf>
- Peltier, T. (2001). *Information Security Risk Analysis*. Auerbach Publications.
- Peltier, T. (2002). *Information Security Policies, Procedures, and Standards*. Auerbach Publications.
- Pethia, R. (2003). Viruses and Worms: What Can We Do About Them? *House Committee on Government Reform, Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census*. Retrieved December 17, 2003, from the World Wide Web: [http://www.cert.org/congressional\\_testimony/Pethia-Testimony-9-10-2003](http://www.cert.org/congressional_testimony/Pethia-Testimony-9-10-2003).
- Polly, J. A. (2001). Learning Right from Wrong. *ON, supplement to Time Magazine, November 2001*, 56.
- Pruitt, S. (2003). Supreme Court Hears Arguments on Internet Filtering Case. *IDG News Service*. Retrieved March 6, 2003, from the World Wide Web: <http://www.computerworld.com/governmenttopstory/0,10801,79058,00.html>.
- PTA. (2001). *Technology Issues as Defined by the PTA Programs*. Retrieved May 5, 2001, from the World Wide Web: <http://www.pta.org/programs/bbesea2003.htm>.

- Quittner, J. (2001). Keeping up with your Kids. *On, supplement to Time Magazine, August 2001*, 26-31.
- Radcliff, D. (2001). Firms Find Porn Close to Home. *Computerworld*, 35(14), 1,73.
- Reuters. (2003). RIAA Threatens Orgy of Lawsuits. *Wired News*. Retrieved July 1, 2003, from the World Wide Web:  
<http://www.wired.com/news/digiwood/0,1412,59391,00.html>
- Richardson, R. (2003). 2003 CSI/FBI Computer Crime and Security Survey. *Computer Security Institute*. Retrieved June 3, 2003, from the World Wide Web:  
<http://www.gocsi.com>.
- Rose, D., & Meyer, A. (1999). *The Future is in the Margins: the Role of Technology and Disability in Educational Reform*. Commissioned by Forum on Technology in Education.
- Rosencrance, L. (2002). FTC Goes after Bait-and-switch Spammers. *Computerworld*, Retrieved April 25, 2002, from the World Wide Web:  
[http://www.computerworld.com/storyba/2000,4125,NAV2047\\_STO70524,70500.html](http://www.computerworld.com/storyba/2000,4125,NAV2047_STO70524,70500.html).
- Sabelli, N. (2001). The Goals Behind the Rhetoric: Why we Don't Always Talk About Technology when we Talk About Technology in Education. *iMP, June 22, 2001*. Retrieved September 5, 2001, from the World Wide Web:  
[http://www.cisp.org/imp/june\\_2001/2006\\_2001sabelli.htm](http://www.cisp.org/imp/june_2001/2006_2001sabelli.htm).
- Sale, K. (2002). Homeschooling. *YAHOO!*, 8(2), 85.
- Salomon, K., Cassat, P., & Thibeau, B. (2003). IT Security for Higher Education: A Legal Perspective. *EDUCAUSE/Internet2 Computer and Network Security Task Force: Dow, Lohnes, & Albertson*. Retrieved March 31, 2003, from the World Wide Web: <http://www.educause.edu/ir/library/pdf/CSD2746.pdf>.
- Sarkar, D. (2002). Net-savvy Students Frustrated. *FCWCOM*, Retrieved August 20, 2002, from the World Wide Web: <http://www.fcw.com/geb/articles/2002/0812/web-pew-2008-2015-2002.asp>.
- Scambray, J., McClure, S., & Kurtz, G. (2001). *Hacking Exposed* (Second ed.). Osborne: McGraw-Hill.
- Scheer, R. (2001). We're Stung by Snoopers' Bugs. *Yahoo! Internet Life*, 7(6), 64.
- Schneider, P. (1999). Charity Begins at Work. *CIO*, 12(22), 44-49.

- Schneier, B. (2000). *Secrets & Lies Digital Security in a Networked World*. New York: John Wiley & Sons, Inc.
- Schulman, A. (2001). The Extent of Systematic Monitoring of Employee E-mail and Internet Use. Retrieved January 9, 2002, from the World Wide Web: <http://www.privacyfoundation.org/workplace/technology.extent.asp>.
- Schulte, B., & Keating, D. (2001). Pupils' Poverty Drives Achievement Gap. *The Washington Post*, pp. A1,A12.
- Schwartau, W. (2001). *Internet & Computer Ethics for Kids (and Parents & Teachers Who Haven't Got a Clue.)*. Seminole, Florida: Interpact, Inc.
- Scott, N. G. (2001). Computers in Education. *iMP*, September 5, 2001. Retrieved September 5, 2001, from the World Wide Web: [http://www.cisp.org/imp/june\\_2001/scott/2006\\_2001scott.htm](http://www.cisp.org/imp/june_2001/scott/2006_2001scott.htm).
- Serim, F. (2001). *From Computers to Community: Unlocking the Potential of the Wired Classroom*. Canada: Centrinity, Inc.
- Shah, N. (2003). Sixth-grader Charged in Grade Switch Caper. *Palm Beach Post*. Retrieved February 19, 2003, from the World Wide Web: [http://www.gopbi.com/partners/pbpost/epaper/editions/friday/martin\\_stlucie\\_e394fc803200526000b.html](http://www.gopbi.com/partners/pbpost/epaper/editions/friday/martin_stlucie_e394fc803200526000b.html).
- Snell, J. (2002). Police take Computer Initiative. *The Oregonian*. Retrieved September 30, 2002, from the World Wide Web: [http://www.oregonlive.com/metrowest/oregonlive.base/metro\\_west\\_news/1032523123238162.xml](http://www.oregonlive.com/metrowest/oregonlive.base/metro_west_news/1032523123238162.xml).
- Sonwalkar, N. (2001). Changing the Interface of Education with Revolutionary Learning Technologies. *Syllabus*, 15(4), 10-13.
- Stallings, W. (2000). *Network Security Essentials*. Upper Saddle River, NJ: Prentice Hall.
- Staniford, S., Paxson, V., & Weaver, N. (2002). How to Own the Internet in Your Spare Time, *Proceedings of the 11<sup>th</sup> USENIX Security Symposium*. Retrieved February 18, 2003, from the World Wide Web: <http://www.cs.berkeley.edu/~nweaver/cdc.web/cdc.web.pdf>.
- Stein, L. D. (1999). The Web is not TV. *WEBTechniques*, 4, 18-20.
- Stoll, C. (2000). *Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage*. Pocket Books.

- Stoneburner, G., Goguen, A., & Feringa, A. (2001). *Risk Management Guide for Information Technology Systems*. Washington, DC: National Institute of Standards and Technology.
- Strauss, H. (2002). New Learning Spaces Smart Learners, Not Smart Classrooms. *Syllabus, 16*, 12-17.
- Swanson, M. (1998). Guide for Developing Security Plans for Information Technology Systems. *Federal Computer Security Program Managers' Forum Working Group: National Institute of Standards and Technology: NIST 800-18*.
- Swanson, M. (2001). Security Self-Assessment Guide for Information Technology Systems. *National Institute of Standards and Technology: NIST 800-26*.
- Symantec. (2003). Symantec Survey Reveals More than 80 Percent of Children Using Email Receive Inappropriate SPAM Daily. Retrieved July 7, 2003, from the World Wide Web: <http://www.symantec.com/press/2003/n030609a.html>
- TechLearning. (2000). TechLEARNING Forum - Internet Filtering--The Debate Continues. *Technology & Learning, 20*(9), 48.
- Tipton, H., & Krause, M. (Eds.). (2000). *Information Security Management Handbook* (4th ed.): Auerbach.
- TSSA. (2001). Technology Standards for School Administrators. *Collaborative for Technology Standards for School Administrators*. Retrieved July 31, 2002, from the World Wide Web: <http://cnets.iste.org/tssa/>.
- Updegrove, D, & Long, M. (2001), EDUCAUSE Task Force on System Security, *NERCOMP 2001: Worcester, MA*. Retrieved February 18, 2002, from the World Wide Web: <http://www.educause.edu/in/library/powerpoint/NCP0107.pps>
- Verton, D. (2002). *The Hacker Diaries, Confessions of Teenage Hackers*. Berkely, CA: McGraw-Hill/Osborne.
- Wadlow, T. (2000). *The Process of Network Security Designing and Managing a Safe Network*: Addison-Wesley.
- Wasserman, E. (2000). Save the children. *The Industry Standard, August 28, 2000*, 110-111.
- WBEC. (2000). *The Power of the Internet for Learning*. Washington, DC: Web-Based Education Commission.
- Woody, C. (2003). Managing the Risk of Internet Connectivity, *Consortium for School Networking 2003: Arlington, VA*. February 26, 2003.

Webb, G. (2001). Sex and the Internet. *Yahoo!*, 7(5), 88-95,136-137.

Zakon, R. (2003). Hobbes' Internet Timeline v6.0. Retrieved February 21, 2003, from the World Wide Web: <http://www.zakon.org/robert.internet/timeline>.