2014

Validating the OCTAVE Allegro Information Systems Risk Assessment Methodology: A Case Study

Corland Gordon Keating
Nova Southeastern University, corland.keating@gmail.com

Validating the OCTAVE Allegro Information Systems Risk Assessment Methodology: A Case Study

by

Corland G. Keating

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

Graduate School of Computer and Information Sciences
Nova Southeastern University

2014

We hereby certify that this dissertation, submitted by Corland Keating, 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 K. Littman, Ph.D. Date
Chairperson of Dissertation Committee

_____ _____

Sumitra Mukherjee, Ph.D. Date
Dissertation Committee Member

_____ _____

Carol C. Woody, Ph.D. Date
Dissertation Committee Member

Approved:

_____ _____

Eric S. Ackerman, Ph.D. Date
Dean, Graduate School of Computer and Information Sciences

Graduate School of Computer and Information Sciences
Nova Southeastern University

2014

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

Validating the OCTAVE Allegro Information Systems Risk Assessment Methodology: A Case Study

by
Corland G. Keating
January 2014

An information system (IS) risk assessment is an important part of any successful security management strategy. Risk assessments help organizations to identify mission-critical IS assets and prioritize risk mitigation efforts. Many risk assessment methodologies, however, are complex and can only be completed successfully by highly qualified and experienced security experts. Small-sized organizations, including small-sized colleges and universities, due to their financial constraints and lack of IS security expertise, are challenged to conduct a risk assessment. Therefore, most small-sized colleges and universities do not perform IS risk assessments, which leaves the institution's data vulnerable to security incursions. The negative consequences of a security breach at these institutions can include a decline in the institution's reputation, loss of financial revenue, and exposure to lawsuits.

The goal of this research is to address the challenge of conducting IS risk assessments in small-sized colleges and universities by validating the use of the Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) Allegro risk assessment methodology at a small-sized university. OCTAVE Allegro is a streamlined risk assessment method created by Carnegie Mellon University's Software Engineering Institute. OCTAVE Allegro has the ability to provide robust risk assessment results, with a relatively small investment in time and resources, even for those organizations that do not have extensive risk management expertise.

The successful use of OCTAVE Allegro was validated using a case study that documented the process and outcome of conducting a risk assessment at George Fox University (GFU), a small-sized, private university located in Newberg, Oregon. GFU has the typical constraints of other small-sized universities; it has a relatively small information technology staff with limited expertise in conducting IS risk assessments and lacks a dedicated IS risk manager. Nevertheless, OCTAVE Allegro was relatively easy for GFU staff to understand, provided GFU with the ability to document the security requirements of their IS assets, helped to identify and evaluate IS security concerns, and provided an objective way to prioritize IS security projects. Thus, this research validates that OCTAVE Allegro is an appropriate and effective IS risk assessment method for small-sized colleges and universities.

Acknowledgements

When starting this dissertation, I did not realize how much of a group effort this would be! Without the indispensable help and support of many others, this dissertation would never have been completed. First of all, I would like to thank the Living God, who has given me strength and perseverance to see this project to its completion.
"Thanks be to God through Jesus Christ our Lord" (Romans 7:25).

I greatly thank the members of my Dissertation Committee, who played such a large role in this process! Dr. Littman provided much valuable input to guide me through this entire degree program. It was through reading Dr. Woody's dissertation that I initially discovered an interest in the topic area for my dissertation. The suggestions by Dr. Mukherjee also were critical for shaping the final product. Thank you!!

I also give a very heartfelt thanks to my contacts at George Fox University, who worked hard to provide an environment for the actual risk assessment project. Even with the loss of a couple of employees, my contacts volunteered their time and energy so that I could complete my research. I especially thank Brad Weldon for his hard work and time spent on this project, when he already had a full plate! I also thank Jared Ocker for his work on this project and giving critical input throughout this process.

I thank the individuals who are experts in the security industry who have given me advice during this dissertation project. Lisa Young offered her expertise in shaping my research, both in directing me toward my final topic and in giving valuable suggestions for the field work. Steffani Burd was a great resource and always encouraged me to finish! Her previous research inspired me; her great feedback helped stay on track. The practical input from Kathleen Roberts was also very helpful. Thank you all!

I also would like to thank the many friends and family members who gave me advice, listened to and encouraged me, and prayed for me along this long road. Thanks to my mom and stepdad, Rex and Marilyn DeChenne, my brothers Jim and Jon, and my sister, Karen, for all their support throughout the years. I cannot name all the precious friends who supported me, but I would like to especially thank Tom Parker, Tom Hancock, David and Sherri Nicolella (with David and Brinley), Dave and Jeanne Snodgrass (with Lauren, Claire, and Grant), Mike and Robin Shapiro, Peri Pierone, and Ginny Snodgrass.

I most likely would not have finished this dissertation if it had not been for my good friend Eric Straw. We went through the Ph.D. process together. We bounced ideas off each other, discussed challenges, spent sequestered weekends writing, and urged the other to not give up. A "true companion!" (Philippians 4:3). Thanks, friend!

Saving the best for last, I would like to thank my wife, Jeanette, for the sacrifices that she has made and for the unwavering support that she has given, without whom this dissertation would certainly not have been completed. She is also an amazing proofreader and secretary. What a woman!! Thanks for being such a great partner! I owe you a long vacation without my computer! I love you.

Table of Contents

List of Tables

Tables

List of Figures

Figures

Chapter 1

Introduction

Background

An information system (IS) risk assessment is the formal process that enables IS risks to be identified and mitigated (Ghernaouti-Helie, Tashi, & Simms, 2011; Liu, Kuhn, & Rossman, 2009; Nikolic & Ruzic-Dimitrijevic, 2009). The risk assessment is designed to identify IS assets and to provide vulnerability and threat descriptions, an approach for classifying risks, and a risk mitigation plan (Nikolic & Ruzic-Dimitrijevic, 2009; Syalim, Hori, & Sakurai, 2009). Numerous methods for performing risk assessments are available, including the *Guide for Conducting Risk Assessments* (National Institute of Standards and Technology [NIST], 2012); *Control Objectives for Information and Related Technology* (COBIT); the *Specification for Information Security Management Systems* (as defined by International Organization for Standardization/International Electrotechnical Commission [ISO/IEC] 27005); and the *Operationally Critical Threat, Asset, and Vulnerability Evaluation* (OCTAVE; Kouns & Minoli, 2010; Landoll, 2011; Liu et al., 2009).

An IS risk assessment is an important component of a comprehensive security plan for any entity, including institutions of higher education (Kouns & Minoli, 2010; Liu et al., 2009; NIST Joint Task Force Transformation Initiative [JTF], 2011). According to Blustain, Chinniah, Newcomb, Plympton, and Walsh (in press), it is vitally important for post-secondary academic institutions to conduct risk assessments to safeguard their institutional data. Blustain, Chinniah et al. (in press) noted that, to establish priorities for

mitigating IS risks, a comprehensive security plan for an academic institution should identify areas that contain the greatest vulnerabilities. Kvavik (2006), in a classic study on the security of Information Technology (IT) in higher education, also noted that post-secondary institutions of all sizes should perform regular IS risk assessments as part of their risk management plans.

According to the classic study on small organizations by Beachboard et al. (2008), validating an appropriate risk assessment methodology for small-sized institutions of higher education has been difficult because many of the current methodologies are complicated. Beachboard et al. noted that commercially developed risk analysis tools, such as RiskWatch®, are expensive and complex and, thus, may result in data quality issues and unreliable risk assessment outcomes. Beachboard et al. also recognized the difficulties encountered by small organizations in applying various non-commercial risk methodologies, such as Facilitated Risk Analysis and Assessment Process (FRAAP), the older OCTAVE-S, as discussed below, and NIST's *Guide for Conducting Risk Assessments* (2012). According to Beranek (2011), it is not feasible to apply IS security management methods developed mainly for larger institutions directly to small- and medium-sized organizations.

OCTAVE Allegro is a popular risk assessment methodology developed in 2007 by researchers at the Carnegie Mellon University (CMU) Software Engineering Institute (SEI), as discussed in the report by Caralli, Stevens, Young, and Wilson (2007), *Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process.* OCTAVE Allegro was developed for the purpose of "identifying, analyzing and prioritizing IS security risks" (Liu et al., 2009, p. 57). Based on the findings of an

OCTAVE Allegro risk assessment, IS professionals are able to identify IS risks and prioritize mitigation efforts by developing security measures to reduce the impact of security incursions (Caralli et al., 2007; Kouns & Minoli, 2010).

Problem Statement

There is a lack of research that has addressed the challenge of conducting IS risk assessments in small-sized colleges and universities, defined as those academic institutions with 4,000 or fewer full-time equivalent (FTE) students (Bougaardt & Kyobe, 2011; Sanchez, Ruiz, Fernandez-Medina, & Piattini, 2010). It is important for small-sized post-secondary institutions to perform risk assessments (Sanchez et al., 2010), yet most risk assessment methodologies have been designed for larger institutions and are not appropriate for smaller ones (Beranek, 2011). Small-sized colleges and universities should use an IS risk assessment methodology that has been proven to work effectively in an environment of their size (Beachboard et al., 2008).

Performance of an IS risk assessment is more challenging in small-sized academic institutions than in large-sized ones due to the small-sized institution's funding limitations and the absence of staff with expertise in the risk assessment arena (Beachboard et al., 2008; Jones, 2009; Yanosky, 2007). In the absence of a practical, reliable, and easy-to-use risk assessment methodology, small-sized colleges and universities typically forego the performance of a risk assessment or conduct a risk assessment that lacks merit (Ewell, 2009).

According to Keating (2012), data collected from 2011 EDUCAUSE Core Data Service's surveys showed that 42% of United States (U.S.) small-sized institutions of higher education performed IS risk assessments on central administrative systems and

data. In contrast, 68% of the largest-sized post-secondary institutions (more than 15,000 FTE students) performed such assessments. Although the number of institutions that perform IS risk assessments has increased over the last five years, it is still the case that fewer small-sized institutions perform IS risk assessments than do their large-sized counterparts (Keating, 2012). Keating's findings are in agreement with the most recent comprehensive studies on information security in higher education performed by the EDUCAUSE Center for Applied Research (ECAR; Kvavik, 2007) and Yanosky (2006). According to Yanosky, the majority of small-sized post-secondary institutions do not employ risk management strategies and seldom, if ever, perform risk assessments. Further, Kvavik, based on his classic ECAR study, stated, "The smaller the FTE [student] enrollment, the less likely an institution is to perform a [security] audit" (p. 66).

Moreover, Beachboard et al. (2008) stated, "Appropriately applying the models [for performing risk analyses] in given organizational contexts represents a daunting task. This is particularly true for . . . small- and medium-sized enterprises" (p. 74). Beachboard et al. also indicated the need to use an appropriate risk assessment approach to "reduce the cognitive and financial burdens associated with conducting reasonably high-quality risk assessments" (p. 75).

If IS risk assessments are not performed regularly as part of a robust risk management program, small-sized academic institutions are increasingly at risk of security incursions (Ewell, 2009) that can result from "vulnerable software, malicious actions, inadvertent user errors, [and] natural and human-made disasters" (Liu et al., 2009, p. 57). Additionally, academic networks that are not adequately secured can be used to launch cyber-attacks on other entities that result in the increase of security incursions at

corporations, government agencies, and other academic institutions (Kvavik, 2006). According to Culnan and Carlan (2009), security breaches at post-secondary institutions and their subsequent negative publicity can lead to a decline in donor contributions as well as financial loss that results from lawsuits.

Dissertation Goal

The goal of this investigation was to examine the effectiveness of OCTAVE Allegro as an IS risk assessment methodology in a small-sized, post-secondary institution in the U.S. The OCTAVE Allegro risk assessment was conducted at George Fox University (GFU), a small-sized private university with approximately 3,500 FTE students and an IT staff of about 20 full-time employees (GFU, 2013b), located in Newberg, Oregon (GFU, 2013a). According to ECAR, a small-sized, post-secondary academic institution is defined as any college or university that has 4,000 or fewer FTE students (Keating, 2012; Smith & Caruso, 2010).

The OCTAVE risk assessment methodology is available in three versions: the original OCTAVE method, OCTAVE-S for small organizations, and OCTAVE Allegro, a streamlined version (Liu et al., 2009). The three versions share common underlying principles, such as being self-directed, being adaptable to an organization's requirements, following a defined process, and focusing on both organizational and technological issues (Caralli et al., 2007; Kouns & Minoli, 2010). Although the original OCTAVE method and OCTAVE-S, developed by Alberts and Dorofee (2003), have successfully been used by larger colleges and universities to perform IS risk assessments (Woody, 2006), these methods are considered too difficult to implement at small-sized institutions of higher education (Al-Ahmad & Mohammad, 2013).

Unlike the streamlined OCTAVE Allegro risk assessment methodology, which can be conducted by one or more IT professionals (Caralli et al., 2007), the original OCTAVE risk assessment is conducted through a series of workshops that require participation by employees from all organizational levels (Alberts & Dorofee, 2003). Inasmuch as ensuring the security of IS resources is a complex task, the team that conducts the original OCTAVE method risk assessment must have extensive knowledge of IS security and risk management (Ekelhart, Fenz, & Neubauer, 2009), including a diverse set of IS security skills and experiences (Kouns & Minoli, 2010).

Although the original OCTAVE method can be used by organizations of all sizes, this methodology was designed for organizations with more than 300 employees (Caralli et al., 2007). OCTAVE-S, a variation of the original OCTAVE method, was introduced by Alberts, Dorofee, Stevens, and Woody (2005) in a document titled, "OCTAVE-S Implementation Guide." OCTAVE-S was designed for smaller organizations with fewer than 100 employees (Alberts et al., 2005). Inasmuch as smaller organizations tend to be less hierarchical than are larger organizations, an OCTAVE-S risk evaluation can be successfully completed by three to five members of an analysis team who have "broad insight into the organization's business and security processes" (Alberts et al., 2005, p. 4). Further, since the analysis team is assumed to have sufficient knowledge of the company's information systems (ISs) and security requirements, there is no need to start the OCTAVE-S assessment process with formal workshops for information gathering as required by the original OCTAVE method (Alberts et al., 2005).

According to Caralli et al. (2007), when compared to the earlier OCTAVE variations, OCTAVE Allegro is designed "to streamline and optimize the process of assessing

information security risks" (p. ix) and, thereby, produces "more robust results without the need for extensive risk assessment knowledge" (p. 4). In contrast to the other versions of OCTAVE, which require involvement from people with substantial security expertise and can take months or years to complete, an organization can utilize OCTAVE Allegro to "obtain sufficient results with a small investment in time, people, and other limited resources" (Caralli et al., 2007, p. ix). The use of the OCTAVE Allegro methodology to perform a risk assessment can help a small-sized college or university in determining IS assets, identifying vulnerabilities and threats to these assets, evaluating risks, and prioritizing risk mitigation strategies (Appari & Johnson, 2010; Caralli et al., 2007) and thereby "quickly improve its risk assessment capabilities" (Caralli et al., 2007, p. 27).

Research Questions

As noted, the goal of this investigation was to determine whether the OCTAVE Allegro risk assessment methodology can be used within the particular constraints of the IT Department at GFU to effectively identify IS risks and prioritize risk mitigation efforts. To this end, the following research questions (RQs) guided this investigation:

RQ1. To what extent is the OCTAVE Allegro methodology sufficiently straightforward for the IT staff at GFU to understand and conduct? (Appari & Johnson, 2010).

Many risk assessment methodologies, such as the original OCTAVE method, COBIT, and ISO/IEC 27005, are complex and require substantial training before an IT professional is able to use the chosen method to conduct a risk assessment. GFU has approximately 20 full-time IT staff members (GFU, 2013b) but currently does not have a dedicated IS risk manager or IT staff with extensive risk management experience, so it is

important for the OCTAVE Allegro method to be easily understood by GFU IT staff (Beachboard et al., 2008; Caralli et al., 2007).

RQ2. To what extent will conducting an OCTAVE Allegro risk assessment help GFU IT staff to identify existing IS assets and classify them in order of importance to the mission of the organization? (Kouns & Minoli, 2010).

One of the first steps in determining IS risks involves identifying IS assets and determining their relative value to the organization; otherwise, efforts can be wasted on analyzing assets that are non-critical to the organization's mission. Outcomes based on conducting the OCTAVE Allegro risk assessment at GFU should provide a clear picture of IS assets in relative order of importance to the business goals of the university (Caralli et al., 2007).

RQ3. To what extent will conducting an OCTAVE Allegro risk assessment help GFU IT staff in identifying and evaluating IS security concerns, including threats, vulnerabilities, and risks in regard to existing IS assets? (Syalim et al., 2009).

Providing a process to identify threats, vulnerabilities, and risks to IS assets is fundamental to an effective risk assessment methodology (Peltier, 2010). Findings from conducting the OCTAVE Allegro risk assessment at GFU should clarify existing risks to GFU's IS assets (Caralli et al., 2007; Liu et al., 2009).

RQ4. To what extent will the completion of a risk assessment using the OCTAVE Allegro methodology provide adequate information for GFU IT staff to prioritize the security measures that should be employed to secure their IS assets? (Peltier, 2010).

The goal of performing an IS risk assessment is to identify important IS assets and to prioritize plans for reducing IS risk for each asset to a level that is acceptable to the

organization (Tohidi, 2011). The performance of an IS risk assessment involves two major stages. The first stage of the risk assessment involves identifying threats to IS assets and vulnerabilities within the IS (NIST JTF, 2011). The second stage involves an analysis of the risk posed to the organization, based on the identified threats and vulnerabilities (NIST JTF, 2011). Analyzing the identified risks, in terms of the potential impact on the organization, enables the risks to be prioritized (Ghernaouti-Helie et al., 2011; Nikolic & Ruzic-Dimitrijevic, 2009). Thus the outcome of the OCTAVE Allegro risk assessment at GFU will provide clarity for IS risk mitigation plans and priorities (Caralli et al., 2007; Grajek, 2013; Liu et al., 2009).

The research method used for this investigation was an exploratory case study, which was conducted at GFU. Consent for the author to conduct the investigation at GFU is presented in Appendix A. According to Sekaran and Bougie (2009), conducting an exploratory study is appropriate when the researcher needs to understand the important factors related to a process, such as a risk assessment in a small-sized university, for which there is little research. Further, Yin (2009) noted that a case study is the most appropriate research method to use when the researcher needs to collect data on pertinent elements of the investigation from the context of an organization, such as a small-sized college or university.

The investigator was able to use the OCTAVE Allegro methodology successfully within the constraints of this small-sized university due to OCTAVE Allegro's streamlined design, potential to produce robust results with a relatively small commitment of time and resources, and ability to be used by IT professionals who lack extensive risk assessment expertise. The results of this research demonstrated the

capabilities of OCTAVE Allegro in conducting an IS risk assessment at a small-sized university.

Relevance and Significance

Relevance

According to the EDUCAUSE/Internet2 Computer and Network Security Task Force (2008), "Academia is recognized as an important resource in our national efforts to improve cybersecurity" (p. 2). Haller, Merrell, Butkovic, and Wilke (2011) also reported that higher education institutions play a key role in helping to solve the problems of cybersecurity. That NIST recently formed the National Initiative for Cybersecurity Education (NIST, 2013) also highlights the significance of higher education in the national cybersecurity issue. Institutions of higher education should be part of the solution to the problem of cybersecurity but, instead, are under threat in regard to their own data. According to Grajek (2013), cyber-attacks against higher education networks are on the increase. Further, reports by Widup (2010) and the Identity Theft Resource Center (ITRC; 2012), show that data breaches at institutions of higher education have exposed millions of personal records in the last few years.

According to Culnan and Carlin (2009), Blustain, Abraham et al. (in press), Groner and Brune (2012), and Jones (2009), additional research in risk assessment in higher education is needed as a means to identify appropriate risk assessment methods, develop security policies, and secure information assets. A classic study by Burd (2006) also indicated that additional research remains necessary to enhance IS risk assessment methods and technologies so that "academic institutions do not become the weakest link in America's information security chain" (Abstract, para. 3).

The EDUCAUSE/Internet2 Computer and Network Task Force (2008) concluded its 2008-2009 Strategic Plan by highlighting the urgency of protecting information assets and safeguarding private records and stakeholder data at colleges and universities. According to the EDUCAUSE/Internet2 Computer and Network Task Force, the development and implementation of "a risk management framework for protecting cyber assets" for colleges and universities is critically important (p. 5). The classic studies by Yanosky (2007) and Voloudakis (2006) indicated that performing an IS risk assessment is an important part of a comprehensive risk management framework. In the absence of a risk assessment, an institution of higher education remains unprepared to fend off or recover from breaches to their IS security.

The relevance of performing a risk assessment also was described by Grajek (2013), who reported that over the past decade information technology security has ranked as a top issue for institutions of higher education. According to Dodge (2009), information systems security breaches at institutions of higher education continue to increase. As noted by Kvavik (2006), a vital concern in addressing IT and IS security is determining whether the institution conducted a comprehensive IS risk assessment. According to Yanosky (2007), performing a risk assessment is a crucial step in enabling a post-secondary institution to recover from potential disasters that could have an adverse impact on ongoing operations.

The relevance of the present research also is supported by Bougaardt and Kyobe (2011) and Groner and Brune (2012), who noted that additional research in the area of risk management for small- and medium-sized entities, such as post-secondary institutions, remains necessary. Importantly, Bougaardt and Kyobe stated that there has

been limited research done to help small institutions “recognise and account for losses from cyber-crime” (p. 167). According to Groner and Brune, existing literature that focuses on the implementation of IS security measures in smaller institutions is limited.

Additionally, in a classic study, Kvavik (2006) emphasized the need to provide a detailed “framework to simplify the risk assessment process” (p. 65) conducted at post-secondary institutions. Kvavik noted that EDUCAUSE supported the development of a risk assessment framework for academic institutions in 2005. However, the current version of the EDUCAUSE initiative only provides “high-level guidance for an effective cyber-risk assessment and management process” (EDUCAUSE/Internet2 Computer and Higher Education Information Security Council, 2013, para. 1).

The EDUCAUSE risk assessment framework includes four phases: Strategic Risk Assessment Planning, Operational Data Collection, Risk Analysis, and Mitigation Planning, and provides the steps that must be performed to complete the assessment. The framework is made for institutions of any size and is meant to be tailored to meet the needs of the institution. Thus, the authors of the framework make clear that those using the framework need to make decisions about which parts of the framework are relevant to a particular situation as well as decide whether parts of the framework should be streamlined for certain situations (EDUCAUSE/Internet2 Computer and Higher Education Information Security Council, 2013).

Due to the EDUCAUSE risk assessment framework’s need to be tailored to fit an institution’s needs, the framework provides only an overview for performing risk assessments; it does not include adequately detailed guidance to enable personnel at small-sized post-secondary institutions to implement effective security solutions or to

properly conduct risk assessments (Beachboard et al., 2008; EDUCAUSE/Internet2 Computer and Higher Education Information Security Council, 2013). Thus, according to Sanchez et al. (2010), there is a need for further research to identify risk management methodologies that meet the particular needs of smaller-sized institutions.

Significance

The significance of this investigation is reflected in the sheer number of institutions that are classified as small and, thus, can benefit from the results of this investigation. According to the latest data collected by the Carnegie Foundation for the Advancement of Teaching (2010), there are approximately 2,500 academic institutions with 4,000 or fewer FTE students. These small-sized colleges and universities comprise just over half of all existing U.S. post-secondary institutions. Thus, the methodology utilized in this study can potentially be used by other similarly-sized institutions (Beachboard et al., 2008).

Barriers and Issues

Culnan and Carlin (2009) noted that, due to the traditional open atmosphere of colleges and universities, ISs in institutions of higher education face more challenges than do commercial businesses when attempting to implement security requirements and perform risk assessments. Similarly, according to Jones (2009), ISs in higher education are built on the premise of a free exchange of information, as seen in academia, and are designed to accommodate a diverse user population. Jones reported that other types of businesses are often able to more stringently control access to information systems, whereas post-secondary institutions must leave data assets more accessible, thus making it more difficult to secure information assets at post-secondary institutions. The

challenge of balancing open access to computing resources with IS security also is recognized by Grajek (2013), who listed one of the top ten IT issues of 2013 as "finding appropriate balance between infrastructure openness and security" (p. 42). According to Luesebrink (2011), the openness and autonomy of campus networks are major barriers to implementing IS security in the academic environment.

Another key barrier to effectively implementing IS security solutions and to performing risk assessments in post-secondary institutions, as identified by Groner and Brune (2012), is the lack of adequate financial and personnel resources. According to Kvavik (2006), absence of IS risk assessments in post-secondary institutions is due to a lack of funding, the absence of skilled security personnel, and the overall perceived difficulty of performing an IS risk assessment. Young (2010) also maintained that post-secondary institutions often do not employ IT staff specifically trained for security management.

As noted above, the general barriers to performing a risk assessment at large-sized colleges and universities include a lack of resources for IT security projects (Grajek, 2013; Groner & Brune, 2012; Ingerman & Yang, 2011), IT staff's inadequate training in IS security (Young, 2010), and the academic culture of openness (Grajek, 2013; Hedrick & Grama, 2013). Research on IS risk management in higher education has tended to focus on larger universities (EDUCAUSE/Internet2, 2013), thereby neglecting the unique needs of small-sized post-secondary institutions. In addition to the above-noted challenges for IS risk management at large-sized institutions, small-sized post-secondary institutions have other challenges, such as an acute lack of funding, the absence of the

required security expertise, and a lack of familiarity with IS security issues (Beachboard et al., 2008; Groner & Brune, 2012).

Limitations and Delimitations

In this investigation, the author conducted a case study at GFU as the IT staff completed an OCTAVE Allegro risk assessment. An OCTAVE Allegro risk assessment can be considered "comprehensive" if an institution analyzes the risks to all important IS assets and develops a risk mitigation plan for every IS asset determined to contain more risk than the organization is willing to tolerate. However, the scope of this study was limited to GFU's development of a risk mitigation plan for the single IS asset that they deem to be most at risk. Therefore, this investigation is not considered a comprehensive risk assessment of all IS assets at GFU. Further, although the long-term value of risk assessments was described by Kouns and Minoli (2010), Landoll (2011), and Peltier (2010), the author did not follow up with GFU after the completion of the case study to determine any long-term benefits to the IS security posture of GFU. As such, the current investigation cannot be considered longitudinal.

Definition of Terms

Information asset (or IS data asset). An information asset includes data (in electronic format or on paper) or other intellectual property that have value for the mission of an organization and that require protection (Alberts & Dorofee, 2003; Caralli et al., 2007; Kouns & Minoli, 2010).

Information asset container (or Container). Any item that holds an information asset (whether for storage, transportation, or processing) constitutes an information asset

container. A container can consist of people, technology, or objects such as paper (Caralli et al., 2007).

OCTAVE Allegro. OCTAVE Allegro is the most recent OCTAVE variation developed by the CMU's SEI for streamlining and optimizing assessments of risks to IS assets, thereby enabling an entity to prioritize risk mitigation efforts. Compared with other versions of the OCTAVE method, OCTAVE Allegro requires less time and fewer staff member resources to complete as well as requires less training for IT staff to be competent to conduct. OCTAVE Allegro focuses its assessment of risk on existing IS assets (Caralli et al., 2007).

OCTAVE Allegro Documentation. The OCTAVE Allegro methodology was first detailed in the 2007 document titled, "Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process" (Caralli et al., 2007). The appendices of that document contain specific steps with detailed activities for performance of the OCTAVE Allegro risk assessment. The OCTAVE Allegro risk assessment process involves the completion of worksheets that are included in the appendices of that document.

OCTAVE Method. The original version of the Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) risk assessment methodology is known as the OCTAVE method. Developed in 1999 by the CMU's SEI, it is typically used by larger organizations (300 or more employees; Alberts & Dorofee, 2003; Alberts, Behrens, Pethia & Wilson, 1999).

OCTAVE-S. OCTAVE-S is an adaptation of the OCTAVE method created by CMU's SEI for smaller organizations (100 employees or fewer), which tend to have a less prominent hierarchical structure than larger organizations (Alberts et al., 2005).

Risk. Risk refers to the potential negative effect to an organization (measured quantitatively or qualitatively) if a vulnerability of an IS asset is exploited by a threat, taking into consideration both the likelihood of the exploitation and the potential severity of impact on the organization (Ghernaouti-Helie et al., 2011; ISO/IEC, 2008; Kouns & Minoli, 2010; Landoll, 2011; Leeden, 2010; NIST JTF, 2012; Ponnam, Harrison, & Watson, 2009).

Risk analysis. A risk analysis is the calculation of the risk, based on the identified threats and vulnerabilities of the organization's IS (Bruijn, Spruit, & van den Heuvel, 2010; Landoll, 2011). The calculation of risk is based on both the likelihood and the impact of a risk's being exploited (Ghernaouti-Helie et al., 2011). A risk analysis is carried out during the process of a risk assessment (Caralli et al., 2007; Kouns & Minoli, 2010).

Risk assessment. Risk assessment is a process that enables IS risks to be identified and mitigated and comprises four overall phases. The first phase of a risk assessment involves identifying both the threats to IS assets and the vulnerabilities in the IS. The second phase concerns determining the actual risk that the threats and vulnerabilities pose to an organization. The third phase of the risk assessment involves an evaluation of the risks and results in identified risks' being prioritized according to organizational impact. The final phase of a risk assessment concerns planning the risk mitigation requirements as a means to bring risk down to a level that is acceptable to the organization (Caralli et

al., 2007; Ghernaouti-Helie et al., 2011; Landoll, 2011; Nikolic & Ruzic-Dimitrijevic, 2009; NIST JTF, 2011; Peltier, 2010).

Risk management. Risk management is a broad term that encompasses the processes associated with framing the risk environment, conducting a risk assessment, analyzing risk, mitigating existing risk, monitoring risk, and conveying information about risk to decision makers and other organizational stakeholders (Ghernaouti-Helie et al., 2011; Kouns & Minoli, 2010; Nikolic & Ruzic-Dimitrijevic, 2009; NIST JTF, 2011).

Small-sized institution of higher education/small-sized post-secondary academic institution. A small-sized institution of higher education refers to a college or university that has 4,000 or fewer full-time equivalent (FTE) students (Keating, 2012; Smith & Caruso, 2010).

Threat. A threat is considered a potential occurrence of an event that produces a harmful outcome to an IS, whether caused by natural events, human attackers, or system errors (Landoll, 2011; NIST JTF, 2012). A threat is realized when a threat source exploits an IS vulnerability (Caralli et al., 2007).

Threat agent/threat source. This refers to a particular source, such as a hacker or disgruntled employee, or situation, such as an act of nature or a system configuration error, that can potentially produce a threat (NIST JTF, 2012).

Threat impact (or impact). The impact of the realized threat event is the tangible and intangible costs to the organization that arise from the exploitation of a vulnerability (Leeden, 2010).

Threat likelihood (or likelihood). The likelihood of a threat being realized is calculated based on the susceptibility of IS vulnerabilities to exploitation and the ability of the threat sources to create the undesired event (NIST JTF, 2012).

Vulnerability. A vulnerability is a potential weakness in an IS, or in the security controls for an IS, that makes an IS susceptible to exploitation by a threat agent. Upon exploitation, a vulnerability can result in a security breach against an entity's IS assets (European Network and Information Security Agency [ENISA], 2010; Ghernaouti-Helie et al., 2011; ISO/IEC, 2009; Landoll, 2011; NIST JTF, 2012).

Summary

The problem investigated in this study was the difficulty of conducting an effective IS risk assessment at a small-sized college or university; this difficulty is due to a lack of personnel with IT security skills and adequate funding for IS security projects. In this regard, there is a need to validate an IS risk assessment methodology appropriate for use at small-sized colleges and universities. The author examined the effectiveness of the OCTAVE Allegro risk assessment's being conducted within a small-sized post-secondary institution. The research method used for this investigation was a case study, which was performed at GFU. (A list of acronyms is found in Appendix B.)

Chapter 2

Review of the Literature

Introduction

In this review of the literature, the author provides a foundation for this investigation (Cone & Foster, 2006; Levy & Ellis, 2006) that specifically involves the performance of a risk assessment of IS assets in a small-sized post-secondary institution (Ingerman & Yang, 2011; NIST JTF, 2011). The first section contains the literature on the importance of IS risk assessment in the overall context of IS security and risk management for organizations and businesses of all sizes. In the second section, the author presents the research on the importance of IS security in higher education and the need to perform an IS risk assessment at post-secondary institutions. The literature in the third section focuses on the current state of IS risk management in small-sized, post-secondary institutions and key challenges that must be addressed in conducting an IS risk assessment in small-sized colleges and universities, such as financial constraints and a lack of IT staff with extensive security expertise (Jones, 2009; NIST JTF, 2013; Yanosky, 2007; Young, 2010). The final section contains literature on OCTAVE Allegro that demonstrates how OCTAVE Allegro's design and features enable this tool to be an ideal IS risk assessment methodology for small-sized colleges and universities (Appari & Johnson, 2010; Caralli et al., 2007).

IS Risk Management

Risk-Based Approach

Allen (2013) maintained that it is unreasonable to attempt to ensure that an IS asset is 100% secure; all risks to information integrity cannot be anticipated or would cost too much in time and resources to eliminate. According to Allen, organizations must employ a risk-based approach to risk management, which is an approach that entails assessing the level of risk associated with IS assets and reducing it to an acceptable level. This risk-based approach enables an entity such as a small-sized college or university to prioritize which security practices are most important to implement to mitigate risk (Allen, 2013). Allen's findings are echoed by other researchers and industry experts, including Ingerman and Yang (2011), Kouns and Minoli (2010), Landoll (2011), and NIST JTF (2011).

In his classic work on risk management, McCumber (2005) noted that experience has "taught both researchers and IT system managers that risk avoidance was simply untenable" (p. 71). Thus, McCumber emphasized the need to employ a risk-based approach to security management as opposed to risk avoidance. In arguing for a risk-based approach, Johnson, Goetz, and Pfleeger (2009) stated, "Perfect security is unattainable, so the goal is risk mitigation, not risk elimination" (p. 49). Further, McCallister, Grance, and Scarfone (2009) maintained that organizations of all sizes should attempt to protect information assets based on the existing level of risk rather than try to remove all risk to all IS assets. The risk-based approach entails the employment of a risk management process (Kouns & Minoli, 2010; Landoll, 2011).

Understanding IS Risk Management

The importance of managing IS risk within organizations is described by NIST JTF (2013), Ghernaouti-Helie et al. (2011), Landoll (2011), Kouns and Minoli (2010), Peltier (2010), and Beachboard et al. (2008). NIST JTF indicated that ISs are subject to serious threats that include "environmental disruptions, human errors, structural failures, and purposeful attacks" (p. 21). Importantly, NIST JTF determined that these threats represent a significant danger to organizations of all sizes and maintained that effective management of IS risk is critically important to protect an organization's core mission and to enable them to maintain their business functions.

Although there are different standards and methodologies that delineate the risk management process, most of the widely accepted standards embrace four or five major phases (Fenz & Ekelhart, 2011). NIST Special Publications (SPs) are widely accepted national standards (Ekelhart et al., 2009; Ghernaouti-Helie et al., 2011; Landoll, 2011). This author conceptualized IS risk management as described in NIST SP 800-39 (NIST JTF, 2011). According to NIST SP 800-39, a comprehensive process for managing IS risk comprises four overarching steps: framing risk, assessing risk, responding to risk, and monitoring risk. In framing risk, an organization decides on an IS risk management strategy based on its assumptions, priorities, and constraints for dealing with risk. The second step is assessing risk, which involves identifying IS threats and vulnerabilities and then determining the risk to the IS posed by these threats and vulnerabilities. The third step of IS risk management is responding to the risk, which involves deciding on and implementing a course of action to reduce the risk to acceptable levels. The fourth step is

monitoring the risk, which allows an organization to observe changes that occur in the risk to the IS and to respond appropriately.

Within the overall risk management process, the central component involves conducting the risk assessment, the outcome of which provides the necessary information to prioritize and mitigate IS risk. According to NIST JTF (2012) the step of assessing IS risk "is one of the key components of an organizational risk management process" (p. 1). Further, Liu et al. (2009) stated that performing an IS risk assessment as part of the risk management process is "critical for identifying, analyzing, and prioritizing IT security risks" (p. 57).

Importance of IS Risk Assessment

According to Yanosky (2007), an effective risk management methodology includes conducting periodic risk assessments. As indicated in Title III of the E-Government Act of 2002 (Public Law 107-347, also known as the Federal Information Security Management Act [FISMA]), an important component of an effective information security program is the periodic completion of a risk assessment (NIST JTF, 2011). Tohidi (2011) found that performing a risk assessment plays a critical role in prioritizing risks and securing IS data. Tohidi's conclusions are in keeping with the findings of Blustain, Abraham et al. (in press), who maintain that performing an IS risk assessment is the foundation for an effective risk management strategy. According to Blustain, Abraham et al., IS security risks must be identified by a risk assessment before these can be properly managed within an institution of higher education.

The importance of performing IS risk assessments by institutions of all sizes also is noted by Beachboard et al. (2008), who stated that conducting an IS risk assessment is a

key element in ensuring effective risk management. Johnson et al. (2009) noted that "accurate risk assessment reduces exposure to unexpected losses and helps price risk more effectively" (p. 47). Moreover, in the latest version of the *National Counterintelligence Strategy of the United States of America*, the National Counterintelligence Policy Board (2009) reported that assessment of human and technological vulnerabilities "is an integral part of the essential and continual task of risk management" (p. 2).

According to Ghernaouti-Helie, Simms, and Tashi (2009) and Ponnam et al. (2009), the main purpose of performing an effective risk assessment is to prioritize security efforts for valuable information assets, such as electronic and physical copies of student and financial information, which are vital to the continued operation of the institution. Because, for most organizations, the cost, in terms of personnel and financial resources, of mitigating all IS risks is impossible (Allen, 2013; McCumber, 2005), it is important to have a method to prioritize risk mitigation efforts. Bruijn et al. (2010) asserted that one of the greatest benefits of performing a risk assessment is that the most significant threats to the institution of higher education can be identified, and cost-effective mitigation decisions that reduce risk to an acceptable level can be made. Thus, an effective risk assessment can help preserve the financial and personnel resources of an organization (Peltier, 2010).

Key Elements of an IS Risk Assessment

Researchers and practitioners have provided various descriptions of the IS risk assessment process. Generally, these investigators, such as ENISA (2012), Ghernaouti-Helie et al. (2011), and Nikolic and Ruzic-Dimitrijevic (2009), include three overall

phases in the risk assessment process: risk identification, risk analysis, and risk evaluation. Other well-respected researchers of risk assessment methods, such as Caralli et al. (2007), Ewell (2009), Landoll (2011), McCumber (2005), Peltier (2010), and Syalim et al. (2009), include a fourth phase, that of risk mitigation planning. This author included risk mitigation planning in the definition of the risk assessment process since risk mitigation is the immediate goal of the risk assessment process (NIST JTF, 2011). The risk identification phase includes developing an inventory of the IS assets controlled by the organization (Caralli et al., 2007; Voloudakis, 2006) and identifying the vulnerabilities of the IS and the threats to the IS (NIST JTF, 2012). Risk analysis involves determining the likelihood of the occurrence of a threat-source that successfully exploits an IS vulnerability and causes a negative impact to the organization. The risk evaluation phase involves prioritizing risks based on the most significant negative impacts that are most likely to occur. Based on these phases of the risk assessment, an organization can prioritize which IS risks need to be mitigated. The outcome of the risk assessment process is to produce a plan for mitigating IS risk to a level that is acceptable to the organization (Ewell, 2009; Peltier, 2010).

The key concepts associated with performing a risk assessment are system vulnerabilities, threats to ISs, likelihood of a threat event that compromises an IS vulnerability, impact of the security breach, risk, and risk analysis (Landoll, 2011; Kouns & Minoli, 2010). These concepts are briefly described in this section and are defined in Chapter 1. The overall risk assessment process includes identifying IS threats and vulnerabilities. A vulnerability is a potential weakness in an IS, or in the security controls for an IS, that, upon exploitation, can result in a security breach against an

entity's IS assets (ENISA, 2010; ISO/IEC, 2009; Landoll, 2011; NIST JTF, 2012). A threat is considered a potential occurrence of an event that produces a harmful outcome to an IS, whether caused by natural events, human attackers, or system errors (Landoll, 2011; NIST JTF, 2012). The agent or situation that can potentially produce the threat is known as the threat source or threat agent (NIST JTF. 2012). A threat is realized when a threat source exploits an IS vulnerability (Caralli et al., 2007).

Risk is measured by a quantitative or qualitative calculation determined by the likelihood of the threat event and the impact on the organization (Kouns & Minoli, 2010; Leeden, 2010; NIST JTF, 2012). A risk analysis is the calculation of the risk, based on the identified threats and vulnerabilities of the organization's IS (Bruijn et al., 2010; Landoll, 2011). The likelihood of a negative event's occurring should be calculated based on the susceptibility of exploitation of the IS vulnerabilities and the ability of the threat sources to create the undesired event (NIST JTF, 2012). The impact of the threat event comprises the tangible and intangible costs to the organization that arise from the exploitation (Leeden, 2010).

IS Security in Higher Education

According to Hedrick and Grama (2013), institutions of higher education, such as GFU, possess large amounts data, "including personal information of employees and students, sensitive institutional business data, and faculty research data" (p. 2). However, as noted by Marks and Rezgui (2009), in contrast to typical businesses, higher education institutions generally provide open access to information resources for students and faculty. Marks and Rezgui noted that allowing open access to large amounts of personal data makes higher education institutions, such as GFU, susceptible to cyber-attacks.

Culnan and Carlin (2009) explained that institutions of higher education, such as GFU, typically have large amounts of computing power and allow access to large amounts of private information through their network and the Internet. The availability of such information over a public network puts university ISs at risk of security breaches. Yanosky (2009) reported that the amount of critical electronic data that colleges and universities have on their networks continues to increase and that this information needs to be protected. Agee and Yang (2009) argue that IT departments in higher education are challenged to find a balance between preventing unauthorized access to personal data and maintaining an atmosphere of open information sharing.

EDUCAUSE reported that, every year from 2003 to 2010, IT departments in higher education have listed data security as one of the top three items considered vital for strategic success (Ingerman & Yang, 2010); in 2011, it was still the fourth most important issue (Ingerman & Yang, 2011). However, from 2009 to 2011, the area of greatest concern to IT departments in colleges and universities involved funding of IT projects and initiatives (Agee & Yang, 2009; Ingerman & Yang, 2010, 2011). According to Ingerman and Yang (2010), security breaches at institutions of higher education continue to increase in severity, and yet the funds to address IS security requirements are scarce. Further, Ingerman and Yang (2010) determined that IS security will continue to be a top concern for institutions of higher education for the foreseeable future.

Data Breaches at Higher Education Institutions

Information stored in the ISs of institutions like GFU continues to be the target of data theft (Collins, Sainato, & Khey, 2011; Marks & Rezgui, 2009; Widup, 2010). According to Collins et al., almost half of all security breaches that were reported in the U.S. in 2005

occurred at institutions of higher education. Collins et al. added, however, that the high percentage of reported breaches was most likely due to the greater reporting transparency in the education sector than in other industry sectors. According to Widup, from 2005 to 2009, a total of 549 data breach incidents occurred at institutions of higher education. These 549 breaches resulted in the disclosure of over 10 million personal records to unauthorized persons. Further, the Identity Theft Resource Center (ITRC; 2011) report for 2010 listed a total of 65 educational sector breaches, resulting in the exposure of 1.6 million records. According to ITRC (2012), in 2011 there were another 59 breaches, with 800,000 records exposed. Thus, there continues to be a significant unintended disclosure of personal information from data contained in higher education ISs.

Culnan and Carlin (2009) described some of the negative consequences that can arise from data breaches in higher education. They noted that, when one large university had five security breaches over a three-month period, the public perceived that the university maintained a lax attitude toward security. Further, the university suffered an 8% decline in donor contributions in the year following the admission of the security breaches and was subjected to lawsuits. Talbot and Jakeman (2009) also reported that IS security breaches can lead to financial losses, legal challenges, and damage to organizational reputation.

Need for Risk Management at Institutions of Higher Education

Ingerman and Yang (2010) indicated that determining the right amount of funding to spend on IS security investments is an important consideration for higher education. Importantly, according to Bruijn et al. (2010) and Peltier (2010), performing a risk assessment can help preserve limited IT funds by identifying the greatest security risks

and prioritizing security measures to prevent incursions resulting from security risks. The prioritization of spending on security-related IT purchases is critical as institutions of higher education struggle with obtaining adequate funding for IT projects and initiatives (Grajek, 2013; Ingerman & Yang, 2011). However, according to Grajek and Arroway (2012), in 2011 fewer than 50 percent of all U.S. institutions of higher education performed a risk assessment on central administrative systems and data. Ghernaouti-Helie et al. (2011) noted that, without the completion of a relevant analysis of IS risk, applied security measures and technologies are ineffective; they will either cause a waste of money or will lead to an inaccurate understanding of the organization's IS security situation.

Ewell (2009) presents a strong case that institutions of higher education must follow a risk management methodology to identify, prioritize, and reduce IS risk, just as non-educational businesses should. Ewell argues that performing a risk assessment is the only way to objectively identify IS risk and use limited IT funds to prioritize which security measures to implement. According to Ewell, colleges and universities must use a dependable risk assessment methodology or the results will not be valid for use by the organization. Without an accurate risk assessment, institutions of higher education will not be able to effectively use their limited personnel and financial resources to secure their ISs.

Jones (2009) conducted an empirical study at a small university to determine the security of IS data at the institution. By viewing existing forms, conducting interviews, observing processes, and collecting data from structured questionnaires, he developed an understanding of the security of personally identifiable information at the university. He

found that the university had some security strategies in place but that they were not fully implemented and, thus, certain faculty, staff, and student information remained vulnerable to security threats. Jones' top recommendation for improving the security at the university was that it should conduct a comprehensive IS security assessment to further identify all vulnerabilities and risks within the institution. Jones felt that the university was overly confident of its security because it was unaware of the vulnerabilities of its IS data and that it needed to conduct a risk assessment.

According to Bruijn et al. (2010), Ewell (2009), and Jones (2009), colleges and universities must perform comprehensive risk assessments on their IS assets so that resources can be prioritized toward the assets at greatest risk of compromise. Without a risk management framework that includes a risk assessment, institutions in higher education will either waste time and money on security measures that do not represent the institution's highest priorities or may have an unfounded or inaccurate view of their security situation. Performance of a proven and repeatable risk assessment methodology, such as OCTAVE Allegro, COBIT, or the Central Computer and Telecommunications Agency's (CCTA) Risk Analysis and Management Method (CRAMM), will provide colleges and universities with an accurate view of IS assets risks and enable the identification and prioritization of security measures that should be implemented. Accordingly, Grajek (2013) maintained that all post-secondary institutions should complete a comprehensive IS risk assessment to help "identify the most-pressing risks and prioritize resources" (p. 44).

Lack of Risk Assessment at Institutions of Higher Education

Despite the need for comprehensive IS risk assessments in institutions of higher education, as noted by Bruijn et al. (2010), Ewell (2009), Ingerman and Yang (2011), and Jones (2009), in 2011 fewer than 50 percent of all U.S. higher education institutions completed an IS risk assessment of central administrative systems and data, such as student financial aid, academic records, and institutional financial information (Grajek & Arroway, 2012). According to Grajek and Arroway, who used comprehensive survey data collected by ECAR in 2011, 68% of U.S. colleges and universities conducted risk assessments of information assets under the control of central IT, such as faculty and staff usernames and passwords. However, Grajek and Arroway noted that only 47% of campuses conducted risk assessments of central administrative systems and data. According to Blustain, Chinniah et al. (in press), it is essential that central administrative systems be subject to comprehensive risk assessments, as they contain the private data of students, faculty, staff, and donors.

NIST JTF (2012) noted that it is critical to monitor IS risks on an ongoing basis. It is not adequate to perform an IS risk assessment at one time and then not continue to monitor its effectiveness and take action based on changes to the IS, institutional priorities, or the threat environment. According to Lang, Grama, Norin, and Workman (2013), the percentage of U.S. colleges and universities where risk assessments of IS assets were performed decreased in 2013 when compared to the previous two years. This decrease indicates that IT departments at higher education institutions are not performing continuous IS risk assessments and, thus, are leaving their IS assets vulnerable to unassessed risks.

IS Security and Risk Management in Small Post-Secondary Institutions

Security and Risk in Small-sized Institutions of Higher Education

Small-sized colleges and universities, those with 4,000 or fewer FTE students (Keating, 2012; Smith & Caruso, 2010), are like their larger counterparts in many ways; they collect customer data, have large amounts of computing power, and allow relatively open access to data (Hedrick & Grama, 2013; Kouns & Minoli, 2011; Sanchez et al., 2010). These institutions have the same responsibility as do large-sized ones to protect customer data and IS assets from cyber-threats. However, these small-sized organizations face additional challenges to safeguarding the integrity of their IS assets (Beranek, 2011; Sanchez et al., 2010). Specifically, smaller-sized colleges and universities usually have fewer financial resources and IT personnel with security expertise than do their larger counterparts (Beachboard et al., 2008; Bougaardt & Kyobe, 2011; Sanchez et al., 2010).

According to Sanchez et al. (2010), using a risk management approach is critical in smaller institutions, just as in larger ones. Yanosky's (2007) classic study noted that performing an IS risk assessment is an important part of business continuity planning and creating the ability for a post-secondary institution of any size to survive an unforeseen disaster. In a classic study of IS security in colleges and universities, Kvavik (2006) also noted that conducting an IS risk assessment was essential to institutions of higher education, regardless of size, a conclusion that is supported by Sanchez et al.

Lack of Risk Assessment at Small-sized Institutions

As noted, the performance of an IS risk assessment is critical for small-sized institutions of higher education (Beachboard et al., 2008; Bougaardt & Kyobe, 2011;

Kvavik, 2006; Sanchez et al., 2010, Yanosky, 2007). Smaller institutions, however, fail to use a risk management method to control IS risk at a far higher rate than do larger institutions. According to a recent ECAR survey of IS security in higher education, only 42% of small-sized institutions reported conducting a risk assessment on central administrative systems and data, such as student records, financial data, and human resources data (Keating, 2012). In contrast, 68% of the largest-sized institutions (more than 15,000 FTE) reported that they conduct risk assessments in regard to such data.

Keating (2012) noted that there is a direct correlation between the size of a college or university and the likelihood of performing an IS risk assessment. As seen in Table 1, data collected from U.S. higher education institutions by the EDUCAUSE Core Data Service in 2011 showed that only 42% of small-sized colleges and universities performed a risk assessment of central administrative systems and data, whereas 55% of medium-sized institutions completed a risk assessment of these assets, and 68% of the largest-sized colleges and universities did so. Similar percentages are shown for performing a risk assessment of data assets administered by an institution's central IT organization; the smaller the college or university, the less likely it is to have performed a risk assessment on these IS assets.

Table 1. IS Risk Assessment Data for Colleges and Universities in 2011 (Keating, 2012)

IS Risk Assessments for all U.S. Colleges and Universities in 2011	Administrative Systems & Data	Central IT Systems & Infrastructure
All Institutions	51%	66%
Small (4,000 FTE or fewer)	42%	58%
Medium (4,000 to 15,000 FTE)	55%	70%
Large (more than 15,000 FTE)	68%	76%

Prior to Keating's (2012) research, the most recent ECAR analyses of risk assessment performance by size of higher education institution were the classic studies of Kvavik (2006) and Yanosky (2007). Findings by Keating about the correlation between the size of the institution and likelihood of performing an IS risk assessment are in keeping with the findings of Kvavik and Yanosky. Kvavik stated, "The smaller the FTE enrollment, the less likely an institution is to perform [a security] audit" (p. 66) or to complete a comprehensive IS risk assessment. Yanosky also reported that smaller institutions were much less likely to complete a risk assessment than were larger institutions.

Challenges of Performing Risk Assessments at Small-sized Institutions

According to Sanchez et al. (2010), most small organizations in the U.S. and the United Kingdom differ from large-sized organizations in that they lack the finances and adequately trained security personnel to perform IS risk assessments. Further, because most widely accepted IS risk management methods were created for larger organizations, small-sized organizations are unable to use these methods to obtain meaningful risk assessment results. For instance, Sanchez et al. maintained that risk management methods such as CRAMM, OCTAVE, ISO/IEC 27005, and COBIT are difficult for small-sized institutions to apply as they require too many resources and are difficult to

administer. Sanchez et al. also noted that the unique characteristics of small-sized institutions beg for the development of a risk assessment methodology designed specifically to meet their needs. A risk management method created for small organizations would have such characteristics as "flexibility, simplicity and cost efficiency (human and time-related)" (Sanchez et al., 2012, p. 425).

Beachboard et al. (2008) and Groner and Brune (2012) found issues in the methodologies available for small- and medium-sized institutions to perform IS risk analyses, such as their being expensive, complicated, and difficult to validate, and thus argued for the need to develop an IS risk assessment methodology that meets the unique needs for small organizations. Beachboard et al., Beranek (2011), and Groner and Brune found that properly applying existing risk analysis models, such as OCTAVE-S (Alberts et al., 2005), ISO/IEC 27005 (ISO/IEC, 2008), and FRAAP (Peltier, 2010) presents an overwhelming task for small organizations due to their lack of security expertise and limited financial resources. Beachboard et al. reported that small-sized organizations are less likely to employ a large IT staff with dedicated security resources or extensive IS security expertise required to apply these IS risk assessment methods.

In addition to Sanchez et al. (2010) and Beachboard et al. (2008), Beranek (2011) also noted the need to create an IS risk management approach designed specifically for small- and medium-sized organizations. The design objectives for an effective IS risk management methodology in small-sized organizations include its not requiring extensive security expertise, ability to document an organization's important IS assets and risks, and being relatively easy to use and low cost (Beranek, 2011; Sanchez et al., 2010). Despite their understanding of these design principles, neither Sanchez et al., Beachboard

et al., or Beranek made mention of OCTAVE Allegro, which is a well-established risk assessment methodology that already has met the design objectives for small-sized institutions by its being easy to use, not requiring security expertise, and effectively allowing an organization to assess IS assets and risks "with a small investment in time, people, and other limited resources" (Caralli et al., 2007, p. ix).

OCTAVE Allegro

The OCTAVE Allegro risk assessment method was first detailed in 2007 by Caralli et al. and published by Carnegie Mellon University's SEI. This document provided an overview of the methodology, detailed instructions on how to perform an OCTAVE Allegro risk assessment, and standardized worksheets that are completed during the risk assessment process. OCTAVE Allegro belongs to the OCTAVE family of IS risk methodologies that have been well accepted both in the research community and in the IS risk management industry (Appari & Johnson, 2010; Kouns & Minoli, 2010; Landoll, 2011; Liu et al., 2009).

As noted, the three versions of the OCTAVE methodology include the original OCTAVE method, OCTAVE-S, and OCTAVE Allegro. These methods share common design principles. Each methodology is self-directed, follows a defined process, is adaptable to the organization that conducts the risk assessment, and focuses on organizational and technological assets (Caralli et al., 2007). The original OCTAVE method was designed for organizations with 300 or more employees (Caralli et al., 2007). Use of the original OCTAVE method requires participants who are very knowledgeable about IS risk management and necessitates a substantial investment of time and effort to successfully complete (Sanchez et al., 2010).

Although OCTAVE-S was designed for smaller organizations of 100 or fewer employees, the use of OCTAVE-S still requires a team of three to five IS risk management experts who have a broad understanding of the IT configuration and security structure of the organization (Alberts et al., 2005). In contrast to the other OCTAVE methods, OCTAVE Allegro is a streamlined process that provides accurate IS risk assessment results with a smaller investment of time and resources and does not require extensive IS security or risk management experience (Appari & Johnson, 2010; Caralli et al., 2007).

Along with OCTAVE and OCTAVE-S, numerous methodologies are currently available for large- and medium-sized organizations to perform IS risk assessments. These methodologies include NIST's Guide for Conducting Risk Assessments (NIST SP 800-30); CRAMM; the Specification for an Information Security Management System (as defined by ISO/IEC 27005); and FRAAP (Beachboard et al., 2008; Beranek, 2011; Kouns & Minoli, 2010; Landoll, 2011; Liu et al., 2009). In contrast to the aforementioned methodologies, OCTAVE Allegro is a streamlined process, requiring less IS security expertise to conduct, and provides standardized worksheets and detailed instructions for doing an IS risk assessment that can be cost-effectively implemented by small-sized post-secondary institutions (Appari & Johnson, 2010; Caralli et al., 2007).

Further, the training requirements to learn the OCTAVE Allegro method are much fewer than for many of the other risk assessment methods available (Caralli et al., 2007). Thus, using the OCTAVE Allegro method would "reduce the training and knowledge prerequisites for participants" (Appari & Johnson, 2010, p. 296). With OCTAVE Allegro, small-sized institutions can "obtain sufficient results with a small investment in

time, people, and other limited resources" (Caralli et al., 2007, p. ix). Moreover, OCTAVE Allegro offers a qualitative risk management approach with an optional quantitative component (Caralli et al., 2007). According to Liu et al. (2009), a qualitative risk assessment is simpler and faster to complete than is a comprehensive quantitative assessment.

The classic study by Dhillon and Torkzadeh (2006) noted that, in addition to addressing the risks associated with technical vulnerabilities, an effective IS risk assessment methodology should identify and address non-technological risks, such as those created by business processes and human factors. The need to address both technical- and process-oriented IS risks is also noted by Holgate, Williams, and Hardy (2012). An OCTAVE Allegro risk assessment highlights vulnerabilities and risks created by the use of technology as well as identifies non-technology-based risks by enabling an organization "to consider people, technology, and facilities in the context of their relationship to information and the business processes and services they support" (Caralli et al., 2007, p. ix).

Caralli et al. (2007) noted that the documentation provided in the OCTAVE Allegro method features standardized worksheets, thereby eliminating the need to purchase expensive documentation or require the expertise to create useful reports. Meaningful results can be obtained by conducting a one-time, comprehensive, institution-wide IS risk assessment or by applying the standardized OCTAVE Allegro worksheets to individual IS assets. By utilizing OCTAVE Allegro worksheets to conduct IS risk assessments of individual assets, a college or university can incrementally build a comprehensive view of IS risks, eliminating the need to overlook other priorities, while taking extended time

to conduct a comprehensive IS risk assessment (Caralli et al., 2007). Thus, the OCTAVE Allegro IS risk assessment method has the features that enable a small-sized college or university to be able to complete a meaningful risk assessment, using limited time and resources.

Summary

The literature presented confirms the importance of using a risk-based management approach for planning IS risk mitigation for organizations of all sizes (Ingerman & Yang, 2011; Kouns & Minoli, 2010; Landoll, 2011; and NIST JTF, 2011). A comprehensive risk management plan includes the periodic performance of an IS risk assessment (Landoll, 2011; Liu et al., 2009) to enable an organization to prioritize its risk-mitigation efforts (Beachboard et al., 2008; NIST JTF, 2011; Tohidi, 2011). The literature on IS security in higher education shows that, in view of the amount of critical data stored on college and university networks, the number of cyber-attacks against these institutions continues to have a significant impact on their ISs (Collins et al., 2011; ITRC, 2011; Widup, 2010). Further, almost half of these post-secondary institutions have never completed a comprehensive IS risk assessment (Bruijn et al., 2010; Grajek & Arroway, 2012). The literature on IS security in small-sized post-secondary institutions shows that most small-sized colleges and universities lack the skills and finances to effectively perform needed IS risk assessments (Beachboard et al., 2008; Sanchez et al., 2010). Overall, the literature confirms the need to identify an appropriate risk assessment methodology, such as OCTAVE Allegro, to meet the unique needs of small-sized colleges and universities (Beachboard et al., 2008; Beranek, 2011; Sanchez et al., 2010). Research also confirms that OCTAVE Allegro is a popularly accepted IS risk assessment

methodology that can successfully be used at small colleges and universities for completing an effective risk assessment (Appari & Johnson, 2010).

Chapter 3

Methodology

Research Design

The author used an exploratory case study for this investigation. According to Sekaran and Bougie (2009), utilization of an exploratory qualitative study is appropriate when additional information is sought to understand the important factors related to a process such as a risk assessment. Further, Yin (2009) noted that, for exploratory research, through which the researcher seeks to understand a phenomenon within its context, a case study is the most appropriate method because it allows the researcher to capture the pertinent elements from the context of an organization, such as a college or university. Importantly, the classic study by Darke, Shanks, and Broadbent (1998) noted that a case study is "the most widely used qualitative research method in information systems research" (p. 273). Darke et al. also observed that case study research is a good tool for researchers who attempt to understand technology-related processes within organizational contexts. Finally, the classic study by Creswell (2003) stated that case study research is an appropriate strategy to use in exploring a process such as a risk assessment.

The OCTAVE Allegro risk assessment methodology has been successfully implemented at companies within various industries, such as state government agencies (Curtis, 2009) and financial institutions (DeSot, 2008; Jenkins, 2009). The purpose of this study was to determine the effectiveness of OCTAVE Allegro in a small-sized university, namely, GFU, located in Newberg, Oregon. Consent for the author to conduct the

investigation at GFU is presented in Appendix A. Prior to conducting this research, the author served as an adjunct faculty member at GFU but currently has no affiliation with GFU.

GFU, a small-sized, independent university with approximately 3,500 FTE students and 20 full-time IT staff members, provided the context for this case study (GFU, 2013a; GFU, 2013b). Yin (2009) indicated that it is appropriate to choose a single case for conducting case study research when the selected institution is representative or typical of other similar institutions. Although the unique study by Schuman (2005) noted that small post-secondary institutions in the U.S. are diverse, he nevertheless chose GFU as one of 12 institutions that are typical of small-sized institutions of higher education in the U.S. Additionally, the selection of GFU was based on the willingness of the IT staff at GFU to participate in the study, as indicated in Appendix A.

When the author initiated contact with GFU in regard to the risk assessment project, GFU had one person assigned to oversee IS security, namely, Mr. Sean McKay, who was the Director of Administrative Computing and operated as Chief Information Security Officer (CISO). Mr. McKay was involved in the initial planning meeting for the OCTAVE Allegro risk assessment at GFU but left employment at GFU before the risk assessment project started. The author worked initially with Mr. McKay and then two other GFU IT staff to complete the risk assessment. Mr. McKay and the IT staff involved in the risk assessment are collectively referred to as "GFU IT contacts." The author interviewed GFU IT staff individuals before and after the risk assessment process and conducted observations of their conduct of the IS risk assessment, including their completing the OCTAVE Allegro worksheets.

Specific Research Method Employed

In this research, the author investigated the extent to which OCTAVE Allegro provided an effective risk assessment methodology for GFU in terms of how much training was required for participants, whether risks to IS assets were identified, and how well GFU was able to prioritize IT security efforts based on the outcome of the risk assessment. Prior to the risk assessment, the author collected baseline data, using the methods described below, including examining archival records, interviewing GFU IT staff, and conducting direct observations. The author also collected data during the risk assessment process and at the completion of GFU's OCTAVE Allegro risk assessment.

According to Yin (2009), a case study involves utilization of multiple sources of data, including a review of archival records and current documentation as well as various data collection methods, including interviews and direct observations. Findings from these multiple sources were corroborated to validate the research conclusions, a process that Yin calls "triangulation" (p. 116). Gillham (2008) also emphasized the importance of triangulation through the convergence of "different kinds of data (or different sources) bearing on the same issue" (p. 29). Gillham stated that a core element of case study research involves this "multi-method approach" (p. 49), which relies on this convergence of evidence from different data sources. The author triangulated the research findings obtained by examining GFU documents and records, conducting interviews of GFU IT staff, and observing GFU IT staff during the OCTAVE Allegro risk assessment process.

Documents

Yin (2009) stated, "Documents play an explicit role in any data collection in doing case studies. . . . there is little excuse for omitting a thorough review of documentary

evidence" (pp. 103-104). Thus, before the OCTAVE Allegro risk assessment was initiated at GFU, the author reviewed all relevant documentation related to the security and risk assessment, including all of GFU's security policies (GFU, 2013b). The author used the information found in these policies, along with other data, described below, to establish a baseline understanding of the IS security stance, risk awareness, and risk mitigation plans at GFU. This baseline was used as a comparison against which to document the changes in GFU's risk awareness that occurred during and at the conclusion of the OCTAVE Allegro risk assessment. At the conclusion of the OCTAVE Allegro risk assessment, GFU's risk awareness, as highlighted by various documents produced during the risk assessment conducted in this investigation, such as lists and values of IS assets, number and types of documented threats and vulnerabilities, and documented risks and risk mitigation plans, was compared to GFU's initial security baseline condition, and the degree of change was determined.

Archival Records

According to Yin (2009), archival records also are an important source of information in case studies. Thus, the author examined existing archival records related to IS security at GFU, which mainly included internally and externally reported security breaches, documents concerning the implementation of security equipment or practices at GFU, and documented malware detection methods used at GFU (Caralli et al., 2007; Peltier, 2010; Whitman & Mattord, 2010).

Interviews

Yin (2009) indicated that interviews are an essential part of any case study. According to Gillham (2008), interviews are "indispensable in case study research" (p. 59). Gillham

also indicated that all interviews fall on a continuum between structured and unstructured, with the structured interviews as more formal in nature. According to Gillham, formal interviews are those that include predefined, structured, or semi-structured questions, whereas informal interviews are those that take place naturally during conversations with participants throughout the case study. The author conducted both formal interviews, using semi-structured questions, and informal interviews to identify details of IS security management at GFU. Formal interviews were conducted before and after the performance of the risk assessment at GFU. Information collected included whether IS assets were prioritized according to their value, how IS asset vulnerability and risk were calculated, how security concerns were identified, how spending on security products was prioritized, and how GFU personnel reviewed and selected security mitigation measures to implement (Peltier, 2010; Whitman & Mattord, 2010). During the interview process, the author sought to determine the GFU IT contacts' understanding of the IS risk situation at GFU, in general, and of specific security-related issues, including their understanding of GFU's mission-critical assets, current vulnerabilities and threats, and risk mitigation priorities.

According to Gillham (2008), interview questions must focus only on concerns that are essential to the investigation and cannot easily be discovered via other means, such as by observation or found in documentation. Yin (2009) further noted that, in a case study, the interview questions must directly relate to the research questions being investigated. The author took these criteria into consideration when developing the interview questions. The formal interview conducted before the performance of the risk assessment was used to provide the author with an understanding of the IS security risk situation at

GFU. The formal interview conducted after the risk assessment was used to address each of the four research questions that formed the basis of this investigation. The semi-structured interview questions used for the pre-risk assessment interview can be found in Appendix C, whereas those used for the post-risk assessment interview are found in Appendix D.

Interviews with GFU IT contacts were conducted both before and after the OCTAVE Allegro risk assessment. The information from initial interviews was used to create a baseline of the GFU IT staff's understanding of the IS risk situation at GFU. The information from the follow-up interview, through measuring the depth of knowledge gained by the risk assessment, was used to evaluate the effectiveness of the OCTAVE Allegro risk assessment at GFU (Yin, 2009).

Observations

According to Yin (2009), collection of relevant data during a case study should include direct observations of behaviors and environmental conditions in the particular setting of the case study. Gillham (2008) stated that observation is "the most direct way of obtaining data" (p. 46) for a case study, based on the fact that it entails observing what people actually do rather than what they say they do. Accordingly, the author observed the risk assessment participant activities that formed the conduct of the OCTAVE Allegro risk assessment process, by being present at group meetings and talking with participants during the completion of OCTAVE Allegro worksheets.

Further, both Yin (2009) and Gillham (2008) recognize the benefits and challenges of being a participant-observer, rather than conducting observations in a structured and detached manner. The nature of this case study required that the author be present during

the risk assessment activities and, thus, take on the role of a participant-observer. Gillham stated that participant observation is the usual way to perform observations in a case study. Gillham noted that, although the observer's presence will have an effect on the activities being performed, the impact on the case study findings can be minimized by the observer's looking for "the probable influence of your presence" (p. 47). Thus, in all observation settings, the author was aware of this "observer effect" (p. 47) and made notes in regard to possible effects on the risk assessment process and outcome.

Scope of Risk Assessment

Yin (2009) described the importance of defining specific time boundaries for the case study. This case study began when the author met, on January 31, 2013, with GFU IT contacts to discuss the scope of the study and ended immediately after the OCTAVE Allegro risk assessment had been completed, on May 23, 2013, on GFU's most valuable IS asset, which is the data in their enterprise resource planning (ERP) system. This study was not designed as a longitudinal study, as the long-term security benefits of conducting an IS risk assessment have been previously documented by Liu et al. (2009), Peltier (2010), and NIST JTF (2011).

The author met with the GFU IT contacts to discuss the scope of the project, the timeline for the risk assessment, and the roles that each person would perform as well as to answer any questions they had. A key component of the OCTAVE Allegro risk assessment process is analyzing the risk for all existing IS assets, along with their value in accomplishing the mission of the organization (Caralli et al., 2007). Risks are then prioritized according to the likelihood of occurrence and the amount of negative impact on the organization if the risk were realized. Based on this prioritized list of risks to

assets, GFU risk assessment participants were able to decide on the most critical asset for which to develop a risk mitigation plan. The case study research continued until the GFU IT staff completed the OCTAVE Allegro risk assessment and produced a risk assessment report and mitigation plan for the single IS asset. The information needed to address the research questions was available after the OCTAVE Allegro risk assessment had been completed on one IS asset.

The OCTAVE Allegro Process

As described by Caralli et al. (2007), the OCTAVE Allegro risk assessment methodology consists of four overall phases that are divided into eight steps. The OCTAVE Allegro Documentation further divides the eight steps into one or more specific activities (Caralli et al., 2007). The OCTAVE Allegro Documentation provides a clear explanation for the completion of the OCTAVE Allegro worksheets, which form the basis of the risk assessment. Completion of the worksheets formalizes the OCTAVE Allegro methodology into an easy-to-follow, repeatable process. The case study at GFU followed these four phases, comprising eight steps, as presented in Figure 1.

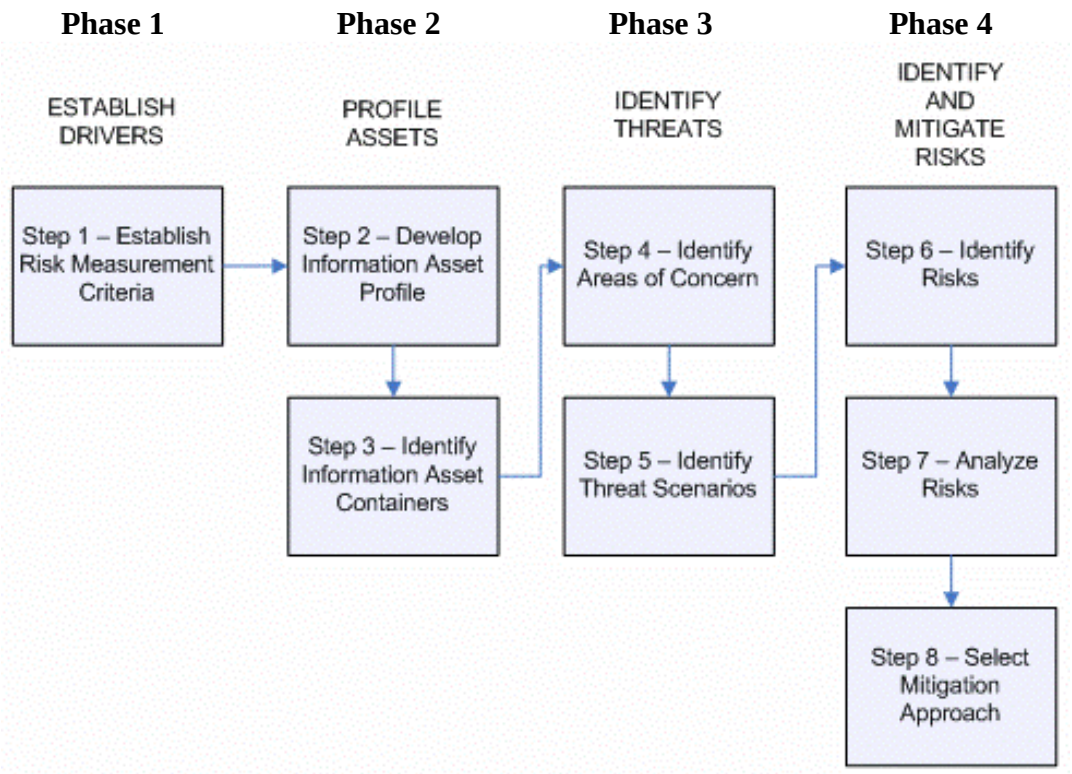


Figure 1. OCTAVE Allegro Roadmap (Caralli et al., 2007, p. 4).

As noted above, according to Caralli et al. (2007), each of the eight steps that form the basis for the OCTAVE Allegro risk assessment contains one or more specific activities. Each activity involves the completion of some part of the OCTAVE Allegro worksheets, which are provided in Appendix B of the OCTAVE Allegro documentation ("OCTAVE Allegro Worksheets v1.0"). The completed OCTAVE Allegro worksheets constitute the final report of the risk assessment for GFU. Table 2 provides an overview of the eight steps of the OCTAVE Allegro risk assessment methodology, with the activities performed in each step. OCTAVE Allegro contains a total of ten worksheets. Table 2 also contains a list of each worksheet (or section thereof) under the activity in which it was completed during the risk assessment at GFU, as instructed in the OCTAVE Allegro risk assessment methodology.

Table 2. OCTAVE Allegro Steps, Activities, and Worksheets (Caralli et al., 2007)

Step	Activities & Worksheets
Step 1: Establish Risk Measurement Criteria	**A1:** Define risk measurement criteria **Worksheets 1 thru 6** - one per organization **A2:** Prioritize the impact areas **Worksheet 7** - one per organization
Step 2: Develop an Information Asset Profile	**A1:** Identify information assets **A2:** Focus on a few critical assets **A3:** Gather info about assets (rationale, description, owners, security requirements) **Worksheet 8** - one per asset
Step 3: Identify Information Asset Containers	**A1:** Identify/Document Containers (technical, physical, people) **Worksheet 9a, 9b, 9c** - one per asset
Step 4: Identify Areas of Concern	**A1:** Threat concerns for each asset/container **Worksheet 10 (sections 1-5)**
Step 5: Identify Threat Scenarios	**A1:** Identify additional threats (technical, physical, people) **(Use Threat Scenarios Questionnaires: Appendix C)** **A2:** Complete Info Asset Risk Worksheet **Worksheet 10 (sections 1-5)** **A3:** Add probability (optional) **Worksheet 10 (section 6)**
Step 6: Identify Risks	**A1:** Determine threat impact **Worksheet 10 (section 7)**
Step 7: Analyze Risks	**A1:** Evaluate consequence **Worksheet 10 (section 8 - Value)** **A2:** Compute relative risk score **Worksheet 10 (section 8 - Score)**
Step 8: Select Mitigation Approach	**A1:** Sort risks into categories **A2:** Assign mitigation approach (Mitigate, Defer, Accept, or Transfer) **Worksheet 10 (section 9)** **A3:** Mitigation strategy **Worksheet 10 (end section)**

Phase 1: Establish Drivers

Phase 1 of the OCTAVE Allegro risk assessment at GFU consisted of Step 1, "Establish Risk Measurement Criteria." This step involved establishing risk

measurement criteria by which to identify and prioritize the most significant security breach impact areas for GFU. The risk measurement criteria constituted "a set of qualitative measures against which the effect of each risk on an organization's mission and business objectives is evaluated" (Caralli et al., 2007, p. 32). These criteria were prioritized from most to least important in terms of greatest potential negative threat impact to the GFU. The security breach impact areas were meant to capture the most important business drivers for the GFU, including the institution's reputation, financial health, productivity capacity, safety and health of employees and clients, and legal obligations (Caralli et al., 2007).

Phase 2: Develop Asset Profile

Phase 2 of the OCTAVE Allegro process consisted of Step 2, "Develop Information Asset Profile", and Step 3, "Identify Information Asset Containers." Step 2 involved identifying and building a profile of GFU's IS assets. The asset profile included a description of each IS asset, the reason each asset was important to the organization, the owner of the asset, and the security requirements for the asset. Step 3 entailed the identification of the locations (referred to as "containers") of the information assets (Caralli et al., 2007). Data asset containers comprise the IT devices in which each data asset was stored and transmitted, the physical locations where the data resided, and the names of individuals who had detailed knowledge of each data asset (Caralli et al., 2007).

Phase 3: Identify Threats

Phase 3 involved the identification of threats to GFU's IS assets and comprised Step 4, "Identify Areas of Concern," and Step 5, "Identify Threat Scenarios." This phase involved identifying possible IS asset threats that could be caused by individuals who

used technology or by physical events, either of which could have a negative impact on the integrity of GFU's IS assets. Physical threats to IS assets can be caused by problems with technology storage, transmission of the asset, or outside events such as adverse environmental mishaps (Caralli et al., 2007). To capture this information effectively, Steps 4 and 5 required two distinct iterations of the threat identification process. Step 4 entailed the identification of areas of greatest threat concern based on previous knowledge or the perceptions of those who conducted the risk assessment. Step 5 then involved performing a more methodical threat identification exercise using threat trees, which were created by filling out questionnaires provided in the OCTAVE Allegro documentation. OCTAVE Allegro recognizes four areas of threats, which it represents as threat trees: human actors using technical means, human actors using physical access, technical problems, and other problems (such as natural disasters; Caralli et al., 2007).

Phase 4: Identify and Mitigate Risks

Phase 4 consisted of the final three steps and entailed the identification and mitigation of risks to GFU's IS assets. Step 6, "Identify Risks", involved the identification of risks, which were determined by considering the consequences of threats being realized and the subsequent impact on IS assets (Caralli et al., 2007). Step 7, "Analyze Risks", was comprised of analyzing the identified risks using a simple quantitative method that prioritized risk based on the relative importance to the institution. Once the risks were prioritized, Step 8, "Select Mitigation Approach", was used to decide which risks needed to be mitigated immediately and which risks could be accepted or mitigation deferred until later. Risk mitigation strategies were then developed for the greatest organizational risks (Caralli et al., 2007).

Validity and Reliability

According to Yin (2009), the quality of case studies can be judged by certain characteristics such as "trustworthiness, credibility, confirmability, and data dependability" (p. 40). Yin described four tests that can be used to ascertain these characteristics: construct validity, internal validity, external validity, and reliability. With the exception of internal validity, each test is relevant and is presented in detail below. Internal validity is a concern only in explanatory case studies that attempt to establish a cause and effect and is not applicable to an exploratory case study, such as this investigation. Nevertheless, the methodology used in this investigation accounted for internal validity by using a convergence of different data sources, such as interviews, observation, and documentation.

Construct Validity

Case study construct validity, as described by Yin (2009), is associated with conducting appropriate procedures for collecting and recording data. Yin described three strategies that can increase the construct validity of the case study. The first strategy is to use multiple sources of evidence, such as interviews, document review, and observations. The second is to follow a procedure that maintains the "chain of evidence" (p. 122). Maintaining a chain of evidence entails keeping records that are detailed to the degree that a subsequent researcher could determine the relationship between the data and the conclusions. The third strategy is to allow respondents to review a draft copy of the results for the purpose of verification. This ensures that keys facts have not been recorded incorrectly or inadvertently omitted. During the data collection and report write-up, the author used these three strategies.

External Validity

Yin (2009) stated that external validity concerns whether the results of a study are generalizable to similar situations. According to Yin, the results of a single-case case study can be generalized beyond the immediate circumstances if the case is considered representative. GFU was chosen as a representative case because it is considered by Shuman (2005) to be one of 12 typical small-sized universities in the U.S. Thus, the risk assessment process at this typical small-sized university can be instructive for similarly-sized institutions (Yin, 2009).

To validate the external validity of this case study, the author gained the assistance of a number of risk assessment experts and practitioners (Appendix E). These experts analyzed the procedures and results of the study to verify the validity of the findings and to determine the generalizability of the case study to other small- and medium-sized institutions.

Reliability

According to Yin (2009), increasing the reliability of a case study will help to minimize any errors in the research and to alleviate any bias of the investigator. A case study can be viewed as reliable if a subsequent researcher could follow the same procedure and arrive at the same conclusions as found by the first investigator. One method to increase the reliability of a case study, as noted by Yin, is for the investigator to maintain a database of evidence collected during the study. The database serves as a repository for all data collected that is kept separate from the final report or conclusions drawn. The author kept a database for this study, which included write-ups from

interviews and observations as well as copies of documents and archival records collected.

Criteria for Interpreting Findings

According to Tohidi (2011), a successful IS risk assessment enables an institution to prioritize the security controls that should be implemented, such as risk mitigation using technology or policies, risk transference using insurance, or risk avoidance. Security controls must be prioritized to utilize limited company resources in the most cost-effective manner. Peltier (2010) noted that a successful IS security assessment will facilitate the identification of IS security concerns and the prioritization of vulnerabilities and ensure the selection of "an appropriate level of control or to accept the risk" (p. 5). Whitman and Mattord (2010) stated that one of the goals of the risk management process is to identify the vulnerabilities of information assets and "to rank them according to the need for protection" (p. 300).

In his classic work on risk assessment, McCumber (2005) noted that, for the risk management process to be successful, it must be cost effective for the institution to perform. Alberts and Dorofee (2003), in their classic work that defined the original OCTAVE method, stated that the tangible outcome of utilizing an effective risk assessment methodology is the assessment report that will guide and prioritize the security measures employed by an organization. Thus, the OCTAVE Allegro risk assessment at GFU was deemed successful, as it met budgetary requirements and provided adequate documentation for the prioritization of security concerns and risks and for the establishment of an effective IS risk mitigation plan (Alberts & Dorofee, 2003; Grajek, 2013; McCumber, 2005).

According to Yin (2009) and Creswell (2003), an important strategy for validating the findings of a qualitative study is to gather data from multiple sources. Thus, the effectiveness of the OCTAVE Allegro methodology applied at GFU was validated by input from a variety of sources, including the IT staff at GFU, industry analysts who are experts at applying risk assessment methodologies, and the author's analysis of the data. After the GFU IT staff conducted the OCTAVE Allegro risk assessment, the author gathered data from the GFU participants via interviews to evaluate whether the risk assessment methodology was successful in their environment. Responses were collected from GFU's IT staff who participated in the risk assessment.

The evaluation of the OCTAVE Allegro risk assessment at GFU was used to answer the four research questions that formed the framework for this investigation. Specifically, the study was evaluated as successful to the extent that answers to the following research questions (RQs) were obtained:

RQ1. GFU IT staff becomes sufficiently familiar with the OCTAVE Allegro methodology to be able to effectively conduct the OCTAVE Allegro risk assessment (Appari & Johnson, 2010; Beachboard et al., 2008; Caralli et al., 2007).

RQ2. GFU IT staff gain an increased understanding of GFU's IS assets, their importance to the mission of GFU, and the extent to which these assets must be protected (Caralli et al., 2007; Kouns & Minoli, 2010; Nikolic & Ruzic-Dimitrijevic, 2009).

RQ3. GFU IT staff gain an increased awareness of specific security concerns in regard to GFU's IS assets, including threats, vulnerabilities, and risks (Caralli et al., 2007; Liu et al., 2009; Peltier, 2010).

RQ4. GFU IT staff demonstrate their skills in prioritizing IS risk management efforts for existing GFU IS assets (Caralli et al., 2007; Liu et al., 2009; Peltier, 2010).

After the OCTAVE Allegro risk assessment was completed at GFU, the author developed a report, found in the following chapters of this study, that details the success of the risk assessment process based on the criteria set forth in the research questions above. The benefits and limitations associated with the utilization of OCTAVE Allegro at GFU also are delineated.

Format for Presenting Results

Yin (2009) suggested that the results of a case study may be clearer to the reader if they are presented in a question-and-answer format. In keeping with Yin's recommendation, the author used a question-and-answer format for the presentation of the case study results, which allowed the author to present how the data gathered related to the propositions under examination. Thus, the report includes a presentation of each research question, followed by a discussion of all applicable data and their meaning in terms of addressing the research question.

Resources

Pilot Site

The researcher conducted the OCTAVE Allegro risk assessment case study at GFU. Mr. Greg Smith, the Chief Information Officer (CIO) at GFU at the start of this research (who subsequently left employment at GFU), indicated to the author that his IT staff would invest the required time and resources to test the viability of the OCTAVE Allegro risk assessment methodology (Appendix A). GFU has approximately 20 IT staff

members, with one staff member designated as the CISO. As noted, the CISO's main title was Director of Administrative Computing and, thus, only part of his responsibilities included directing GFU's IT security efforts (GFU, 2013b). The CISO was involved in the initial planning meeting for the OCTAVE Allegro risk assessment at GFU. However, the CISO left GFU before the actual risk assessment project was initiated.

Two participants performed the OCTAVE Allegro risk assessment at GFU; both were male employees of the GFU IT department. Although there was no acting CISO at GFU during the main part of this investigation, this did not substantially affect the OCTAVE Allegro risk assessment. The main participant who performed the risk assessment shared security responsibilities with the former CISO. Further, the OCTAVE Allegro methodology does not require that the participants have prior risk management experience or knowledge for successful completion.

Risk Assessment Experts

To confirm that the OCTAVE Allegro risk assessment was performed properly at GFU and that this research is generally applicable to other small-sized post-secondary institutions, the author obtained input from experts in implementation of OCTAVE Allegro and the risk assessment process. The author contacted the security risk experts listed below, who provided input on the risk assessment process, research design, and guidelines for addressing the effectiveness of the risk assessment at GFU. These individuals also commented on the extent to which the risk assessment results can benefit other small-sized post-secondary institutions, as indicated in Appendix E.

- Lisa Young, co-author of the OCTAVE Allegro method and an employee of the CMU's SEI.

- Steffani Burd, Ph.D., a risk management expert and author of the U.S. Department of Justice's report on security in higher education, "The Impact of Information Security in Academic Institutions on Public Safety and Security" (National Criminal Justice Publication No. 215953; Burd, 2006).

- Kathleen Roberts, Founder and Principal of iSecure Solutions, which specializes in performing risk assessments for small-sized colleges and universities.

Software

OCTAVE Allegro includes detailed worksheets that can be replicated to support performance of the IS risk assessment (Caralli et al., 2007). Importantly, the CMU's SEI has validated Digital Defense Inc.'s creation of the proprietary "Enterprise Risk Assessment Utility" (popularly referred to as the "ERA Utility") software program as an electronic implementation of the OCTAVE Allegro risk assessment worksheets (Digital Defense Inc., 2009). This software utility enables a user to electronically record the information collected during the risk assessment rather than to write the results on multiple printed forms. Use of the ERA Utility expedites the paper management process and streamlines the procedures necessary for producing the final OCTAVE Allegro report. The author attended the official OCTAVE Training course (SEI Training, 2013), where he obtained a copy of the ERA Utility software for implementation at GFU. GFU used the ERA Utility to facilitate all data collection during the risk assessment process.

Summary

This chapter presented the methodology that was used in this exploratory case study conducted at GFU. To create a baseline of GFU's IS security posture, security documentation and archival records were collected by the researcher prior to the commencement of the risk assessment. Data also were collected from interviews of the

GFU IT staff and direct observations of the GFU IT staff as they conducted the OCTAVE Allegro risk assessment.

The performance of the risk assessment followed the four phases, composed of eight steps, of the OCTAVE Allegro methodology, as described by Caralli et al. (2007). To ensure the validity and reliability of the case study, the author followed various practices, as described by Yin (2009), including the use of multiple sources of data, comprised of interviews, documentation, and observations, to corroborate research findings. Construct validity was strengthened by maintaining a connection between the data collected and the conclusions drawn. The author allowed key GFU IT staff to view a draft copy of the case study to ensure that key facts were included. External validity was maintained by allowing risk assessment experts, including Lisa Young, Steffani Burd, and Kathleen Roberts, to review the findings. Finally, to ensure reliability, the author maintained a database of all evidence collected during the case study.

To determine the success of this investigation, the findings of the GFU risk assessment were used to address the research questions. The author believes that the OCTAVE Allegro risk assessment was sufficiently easy for GFU IT staff to understand and conduct and that the completion of the risk assessment provided GFU with a better understanding of their IS assets as well as enabled them to create effective risk mitigation plans and to prioritize their IS security spending. The results of this investigation are presented below in a question-and-answer format. Specifically, the report of this investigation includes a presentation of each research question, followed by a discussion of all applicable data and their meaning in terms of addressing the research question.

Chapter 4

Results

Introduction

The purpose of this chapter is to present the results of this investigation. The chapter begins with an overview of the data collection process, including a change that occurred in the GFU IT department that affected the resources available for conducting the risk assessment. Then, detailed findings from the risk assessment case study are presented in a question-and-answer format as they relate to the four research questions. The chapter concludes with a summary of the results.

As noted, Yin (2009) and Gillham (2008) stated the importance of collecting various types of evidence for a case study, including relevant documents, archival records, notes from observations, and answers from formal and informal interviews. Each of these types of data was collected before, during, and after the risk assessment process, as detailed below. The initial data collected before the start of the risk assessment formed the baseline of the IS risk investigation at GFU against which to compare the data collected at the end of the study.

To ensure the construct validity of this study (Yin, 2009), the two GFU risk assessment participants were given a draft copy of these results to verify that what was recorded in the results represented their situation accurately. After reading this report, Participant 2 (who acted as the interim Director of Administrative Computing) validated the accuracy of data gathered during the risk assessment process and stated that it was a fair assessment of the security situation at GFU.

At the start of the OCTAVE Allegro risk assessment investigation, the author created a baseline of the initial IT security situation at GFU. This baseline was created from information gathered during the initial meeting with GFU IT contacts, by conducting a formal pre-assessment interview, gathering all existing IT security documents, and collecting IT security archival reports. During the risk assessment, the author took detailed notes based on direct observations of the risk assessment process, viewed documents produced by the participants during the risk assessment project, and conducted informal interviews with the two risk assessment participants. At the end of the project, the author conducted a formal post-assessment interview with Participant 1, who performed the majority of the risk assessment. The author also collected documentation related to the project, including copies of completed OCTAVE Allegro worksheets. Due to confidentiality concerns at GFU, these documents are not included in this investigative report.

According to Yin (2009), the preferred strategy for analyzing case study evidence is to rely on the theoretical propositions that formed the basis of the study. Yin also stated that the results of the case study can be presented in a question-and-answer format, which allows the author to organize the data according to the propositions that are being examined in the study. Thus, the author presented and analyzed the data collected in this investigation according to their relationship to the research questions.

As the risk assessment project was to begin, two of GFU's senior IT managers left GFU to take positions at other institutions, which left GFU without a CIO or a Director of Administrative Computing (who also held the title of CISO). Inasmuch as the existing staff filled in for two staff members, the remaining GFU employees could not commit the

full amount of time to the risk assessment project, as originally planned. Nevertheless, GFU IT staff and senior management wanted to move forward with this investigation. The IT staff and senior management understood the importance of performing a risk assessment of IS assets but were able to do only a scaled-back version of the project. The acting IT managers decided that GFU's IT staff could dedicate a total of only 40 hours of the network administrator's time, over a period of two weeks. GFU IT staff completed as much of the risk assessment as could be done in that time, and used this project to determine how useful OCTAVE Allegro could be to GFU as a long-term component of their IT security efforts and reporting mechanisms. The network administrator chosen to perform the bulk of the risk assessment had worked at GFU for approximately 14 years. This individual is referred to in this report as Participant 1. This individual had a good understanding of the network, IS assets, and GFU computer users' needs.

Results Related to RQ1

The first RQ is, To what extent is the OCTAVE Allegro methodology sufficiently straightforward for the IT staff at GFU to understand and conduct? The results related to this question are presented in the material that follows.

The Baseline Situation

The first topic addressed through an analysis of the case study data is the extent to which the OCTAVE Allegro methodology was sufficiently straightforward for the IT staff at GFU to understand and conduct. GFU IT participants stated that, before the risk assessment case study project started, their IT staff had no previous knowledge of or experience with the OCTAVE Allegro method and very little knowledge of any risk

assessment methods. In the initial interview, GFU IT contacts said that GFU's IT staff had not previously performed an IS risk assessment.

Initial Training

The amount of training received by GFU IT participants before the start of the OCTAVE Allegro risk assessment project was minimal. Participant 1 stated that, before the project started, he spent about four or five hours reading about OCTAVE Allegro, reviewing online documentation of how other people had used OCTAVE Allegro, glancing through the OCTAVE Allegro Documentation (Caralli et al., 2007), and twice listening to an 18-minute podcast by Lisa Young (Young & Allen, 2008), which provided an introduction to the OCTAVE Allegro method and how it can be used in organizations. He noted that he was trying to get the overall picture of how a risk assessment could be used in their environment but that the podcast did not give him particular knowledge of the specifics of applying the OCTAVE Allegro methodology. He also stated that he did not read any parts thoroughly. As noted, "Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process" by Caralli et al. (2007) was the SEI document that introduced OCTAVE Allegro and provided an explanation of how to perform a risk assessment using this methodology.

At the start of the risk assessment project, the author met with the two GFU risk assessment participants and spent about two hours with them, providing informal training. The training consisted of their reading the appendices of the OCTAVE Allegro Documentation and the author's providing information as needed. Each of the eight steps of the OCTAVE Allegro process includes one or more activities, and each is explained in detail in the OCTAVE Allegro Documentation Appendix A ("OCTAVE Allegro Method

Guidance v1.0"). Every OCTAVE Allegro activity involves the completion of a certain section of one of the ten OCTAVE Allegro worksheets. The worksheets are found in the OCTAVE Allegro Documentation Appendix B ("OCTAVE Allegro Worksheets v1.0"). The relationship between the eight OCTAVE Allegro steps and the ten worksheets are presented in Table 2, above. A printout of Table 2 was given to each risk assessment participant during the informal training session.

During the initial informal training, for each of the eight steps, the author and the two risk assessment participants first read the explanation found in the OCTAVE Allegro Method Guidance v1.0, which describes the different activities related to the step. The participants then looked at the corresponding worksheet(s) in the OCTAVE Allegro Worksheets v1.0, followed by reading the completed worksheet examples found in the OCTAVE Allegro Documentation Appendix D (OCTAVE Allegro Example Worksheets v1.0). (When the participants read about Step 5, the participants briefly looked at the questionnaires found in Appendix C of the OCTAVE Allegro Documentation [OCTAVE Allegro Questionnaires v1.0], which are meant to simplify the Activities in that step.) The participants followed this process for each of the eight steps, reading the OCTAVE Allegro Method Guidance v1.0, while looking at the OCTAVE Allegro Worksheets v1.0 and then viewing the corresponding examples in the OCTAVE Allegro Example Worksheets v1.0.

As noted above, Step 1 entailed the establishment of risk measurement criteria for GFU. Before the start of the risk assessment project, Lisa Young (co-author of the OCTAVE Allegro Documentation) gave the author some additional information to help with Step 1 of the OCTAVE Allegro risk assessment (Appendix F). Young suggested

that GFU try to make the risk measurement criteria as quantitative as possible, setting numeric thresholds to separate the low-, medium-, and high-risk measurement categories. She also said that experience has taught that it is best to set "Teaching Time" as another risk management criterion for institutions of higher education (in the User Defined category, Worksheet 6). The author presented an overview of these further instructions to the GFU risk assessment participants during the informal training process and distributed a printed copy of Young's email so that this information could be incorporated into the risk assessment project.

Based on this training, the GFU IT contacts started to engage in Step 1 of OCTAVE Allegro, filling out Worksheets 1 through 7. During this process, the author pointed out that it would be helpful to look at the examples in the OCTAVE Allegro Example Worksheets v1.0 to understand specifically what was expected in completing Step 1 activities. Thus, the two risk assessment participants decided to fill out Worksheets 1 through 7 to the best of their knowledge. The participants set categories and suggested dollar amounts and percentages but realized that it would be important to obtain input from the Chief Financial Officer (CFO), who also was the acting CIO, to accurately fill in dollar amounts and complete the prioritization required on Worksheet 7.

Formal and Informal Interviews

The day after the informal training, the author asked each GFU risk assessment participant how easy they felt OCTAVE Allegro was to understand and use, based on what they had seen so far. Participant 1 said that it looked fairly easy to use. Participant 2 stated that OCTAVE Allegro seemed pretty straightforward, based on what he had seen. There were no areas that caused him concern or that seemed too difficult to

understand. He stated that the documentation seemed to have the appropriate amount of detail to enable someone to walk through all the major steps of the risk assessment.

In a formal interview after the risk assessment was complete, Participant 1 was asked how understandable he found OCTAVE Allegro to be and what parts he found difficult to understand. Participant 1 responded that it was fairly understandable and that it was very helpful to see the examples in the OCTAVE Allegro Example Worksheets v1.0. He said that his understanding of the whole process would most likely have been significantly harder without having the examples to view. These examples helped this respondent understand the purpose of each activity.

Observations

Throughout the risk assessment process, Participant 1 often demonstrated that he was able to understand the OCTAVE Allegro process fairly easily, based on reading the explanation of the activities and viewing the examples in the OCTAVE Allegro Documentation. Notably, immediately after reading the OCTAVE Allegro Documentation, the two risk assessment participants started entering information in Worksheets 1 through 7, as noted. Another example of their understanding was seen when the participants began Steps 2 and 3 for the OCTAVE Allegro process. After Participant 1 reviewed the OCTAVE Allegro Method Guidance v1.0 of the OCTAVE Allegro Documentation and viewed the examples in the OCTAVE Allegro Example Worksheets v1.0, he was able to immediately start completing the worksheets. When Participant 1 would have questions about what a particular item meant, he would go back to review the examples in the OCTAVE Allegro Example Worksheets v1.0; this often put

him back on course, when he started to go off course, and answered any questions that he had.

Another demonstration of the straightforward and understandable nature of the OCTAVE Allegro instructions was when the participants were called upon to describe the process to others. According to the OCTAVE Allegro Documentation, the information recorded in Step 1 (Worksheets 1 through 7) should reflect the risk tolerance levels of the university's management team. Thus, during the first week of the risk assessment, the participants met with the CFO to complete OCTAVE Allegro Worksheets 1 through 7. The participants had previously completed these sheets so that they would be ready for the CFO to fill in specific dollar amounts and percentages. To start the meeting, Participant 2 explained that levels of risk were to be established for the university, based on risk factors such as reputation or financial costs, as shown in the worksheets. The CFO readily understood the intention of the exercise and immediately began to fill in percentages and dollar amounts for low-, medium-, and high-risk factors for each category. Near the end of the meeting, the CFO asked whether the prioritization in Worksheet 7 was about university-wide priorities or just for the IT department. When neither of the two GFU participants offered to answer, the author clarified that these priorities were for the whole university and explained that, if GFU's Risk Department already had established risk priorities, those could be used instead of this OCTAVE Allegro worksheet.

Near the end of the of the risk assessment project, another opportunity arose for Participant 1 to explain the OCTAVE Allegro process, which demonstrated how well he understood the entire method. The final step of the OCTAVE Allegro risk assessment

(Step 8) required that priorities be set for different IS asset risks. Participant 1 had been performing the day-to-day activities of the OCTAVE Allegro risk assessment but wanted Participant 2's input during this prioritization process. To explain the results of the risk assessment up until that point, Participant 1 gave an overview of the entire OCTAVE Allegro risk assessment process and explained how input was needed for Step 8. Based on the author's observation, he appeared to give an accurate overview of the process without needing input from any documentation. Participant 1 then explained to Participant 2 that, during the risk assessment, they had only one threat identified per asset. However, if GFU's IT staff took time to complete more threat scenario worksheets, the assessment would show multiple threats listed for each IS asset. Having multiple threats documented would provide a more complete picture of GFU's risk situation and aid in their security decision making and prioritization.

Documentation

GFU's IT participants' ability to understand the OCTAVE Allegro process was demonstrated by their ability to produce a complete and meaningful risk assessment final report within a very short timeframe. The clearly delineated activities related to each step as detailed in the OCTAVE Allegro Documentation allowed the participants to read, understand, and focus on one task at a time, filling in the information required for each of the successive worksheets. This process allowed participants to incrementally produce a finalized risk assessment report.

Results Related to RQ2

The second RQ is, To what extent will conducting an OCTAVE Allegro risk assessment help GFU IT staff to identify existing IS assets and classify them in order of

importance to the mission of the organization? The results related to this question are presented in the material that follows.

The Baseline Situation

The second topic to be addressed by an analysis of the case study data is the extent to which conducting an OCTAVE Allegro risk assessment helped GFU IT staff to identify existing IS assets and to classify them in order of importance to the mission of their organization. In the pre-risk assessment interview, the GFU IT contacts stated that the IT staff did not keep a list of their IS data assets or maintain documentation on which computer systems stored or transmitted these assets. GFU's IT department controls and maintains the systems on which all IS assets are stored, monitors access to these data, and supports faculty and staff who use these IS assets. Thus, the GFU IT staff knows which assets exist and where they were stored and processed in general terms, and has an intuitive feel for their value to the organization, but this was not formally documented. Each IT staff member works with different IS assets and systems and, thus, would have more knowledge about some IS assets and less about others. There was no comprehensive view of GFU's IS assets, how they were stored and transmitted, or their value to the organization.

Formal Interview

In the post-risk assessment interview, Participant 1 was asked whether he felt that the OCTAVE Allegro process helped him to identify existing IS Assets. Having worked in the IT department at GFU for 14 years, Participant 1 felt that the OCTAVE Allegro process did not substantially help him understand what IS assets existed, as he already was familiar with them. He did note, however, that it was helpful to talk to the data asset

owners about how each asset was used. After a number of conversations with data asset owners, Participant 1 realized that he had an incomplete view of the IS assets from the perspective of who accessed the data, where the data were accessed from, the devices used to access and store the data, the full extent of their security requirements, and what security controls were already in place. The OCTAVE Allegro process helped him to achieve a more comprehensive view of the IS data assets.

Participant 1 also was asked, in the post-risk assessment interview, whether the OCTAVE Allegro risk assessment helped him to classify the IS assets in terms of importance to the organization. He stated that he already knew the importance of the assets and, thus, the risk assessment did not substantially help in that regard. He did, however, gain valuable insights from interviews with the data owners with whom he spoke. He did not interview all IS asset owners, as he ran out of time for the project. He thought that, if he did interviews with all the data owners, this would have brought out valuable information as to the importance and value of the different IS assets.

Informal Interviews

The author's informal talks with Participant 1 during the risk assessment provided insight into how the OCTAVE Allegro risk assessment helped to identify the details of GFU's IS assets, such as the security requirements for each data asset. On the second day of the risk assessment, Participant 1 spent time filling out Worksheet 8 for Step 2, which entailed the development of an Information Asset Profile. Although Participant 1 was able to complete much of the worksheet from information he already knew, on the third day of the risk assessment, he had still not completed Worksheet 8 for all assets; he said that he wanted to talk to more of the data owners to obtain a better understanding of the

security requirements for different assets. After talking with the various data owners, Participant 1 was able to complete that section of the Information Asset Profile.

Other conversations with Participant 1 confirmed that performing the OCTAVE Allegro risk assessment helped him to identify the containers in which the data assets are stored, processed, and transmitted. On the third day of the risk assessment, Participant 1 started working on Step 3 (Worksheet 9), which involved identifying the containers of each IS asset. After working on this for about two hours, Participant 1 realized that he needed to talk to the owners of various data assets to obtain a better understanding of the containers in which data were stored and processed. After each conversation, he was able to complete more of the Information Asset Profile and, thus, obtain a more complete view of the data assets.

The process of documenting detailed information about each IS data asset proved to be helpful in identifying data ownership and responsibility. For instance, in documenting the data assets (Worksheet 8), Participant 1 realized that, as far as he knew, the responsibility for compliance to the Payment Card Industry Data Security Standard (PCI DSS) for some of their data was not clearly delineated. Participant 1 noted that this responsibility for PCI DSS compliance was something that needed to be addressed.

Observations

Participant 1 wrote down most of GFU's important IS assets from memory. Although Participant 1 knew all the GFU IS assets that existed within IT's control, in the process of remembering and capturing all this information in the OCTAVE Allegro worksheets, he had to go through a brainstorming process. While working to write down all of the important IS assets, Participant 1 looked through the administrative department areas on

the GFU public website. The website helped Participant 1 realize that he had forgotten to include the GFU email system and the student health information data in the list of IS assets. He eventually identified a total of ten different IS assets.

After Participant 1 had identified these ten IS assets, he gave them an informal ranking, based on his perception of which were most important to the university. He quickly came up with five different levels of importance and placed the data assets in these categories. Three of the IS assets were placed in category one, indicating that these assets were the most important to GFU.

Documentation

The tangible output from the OCTAVE Allegro risk assessment at GFU was a report that consisted of the completed OCTAVE Allegro Worksheets. Included in this report was a detailed list of all IS data assets as well as descriptions of how the data were used, who owned the data, the security requirements for the data, and where the data assets were stored, processed, and transmitted. Due to the participants' completing the OCTAVE Allegro risk assessment, GFU now possesses a comprehensive description of their IS assets, which includes written security requirements, something that did not previously exist in written form.

Results Related to RQ3

The third RQ is, To what extent will conducting an OCTAVE Allegro risk assessment help GFU IT staff to identify and evaluate IS security concerns, including threats, vulnerabilities, and risks in regard to existing IS assets? The results related to this question are presented in the material that follows.

The Baseline Situation

The findings presented here concern the extent to which conducting the OCTAVE Allegro risk assessment helped GFU IT staff to identify and evaluate IS security concerns, including threats, vulnerabilities, and risks, in regard to existing IS assets. In the author's initial meeting with GFU IT staff, the CISO said that GFU's IT staff plan and operate their IT security-related activities intuitively; the IT department has no methodology in place to objectively validate the need for GFU's IT security operations. Based on an initial look at OCTAVE Allegro, the CISO was excited about what the risk assessment could do for GFU's IT department in terms providing a formal method to validate GFU's security-related IT efforts.

The CISO also said, in the initial meeting, that GFU did not have a written security response document. The IT staff did have an informal plan and understanding of the steps that they follow when confronting a possible security breach, but these steps were not documented. Most of the IT staff has worked at GFU for many years, and IT management has a high level of trust in their IT employees and believes that GFU's IT staff members all have a good understanding of GFU's informal security processes. Nevertheless, the IT staff hoped to document their security response process at some point.

In the pre-risk assessment interview, the GFU IT staff members stated that the IT department seldom did any type of vulnerability analysis or scan of IT assets. IT staff members would run a vulnerability scan only if there were a specific reason to do so, for example, if their network monitoring tool indicated that there were some open Internet Protocol (IP) ports on a piece of equipment such as a printer. The IT staff members also

indicated that GFU did not regularly perform penetration testing or have a process for calculating IS asset vulnerability and risk.

GFU IT staff keeps a spreadsheet that lists reported or known security incidents. The list includes a description of the incident or problem, who was involved, what equipment was involved, the security team that handled the incident, and what the resolution was. As of May 1, 2013, the spreadsheet included 26 incidents, ranging from June 24, 2010, to April 26, 2013. Many of the incidents included unwanted incoming or outgoing traffic from open IP ports on computers or other equipment. There were a number of denial-of-service attacks against the GFU Newberg Campus. There were various other incidents that included employees' emailing employee social security numbers in plaintext, requests to access an employee's email account, and reports of publicly listed passwords as well as stolen computers.

Formal Interview

In the post-risk assessment interview, Participant 1 stated that the OCTAVE Allegro risk assessment would have been very useful for identifying and evaluating IS security concerns if the participants had spent more time on Phase 3 of the assessment (Identify Threats). As it was, the participants mostly identified and documented threats and vulnerabilities of which GFU's IT staff were already aware, based on the limited amount of time that the participants had to spend on the risk assessment project. GFU's IT staff members did not use this iteration of the risk assessment mainly as a tool to identify other threats but, rather, to validate OCTAVE Allegro's usefulness as a security tool for GFU. The participants are aware that there are other threats that were not completely addressed by this risk assessment. For instance, at one point in the risk assessment process, the

GFU participants mentioned that they were unaware of whether paper copies of student information were being properly protected; this potential risk has not yet been addressed or documented.

Informal Interviews

Various conversations during the risk assessment project shed light on the value of OCTAVE Allegro in terms of helping to identify IS threats and analyze their risks. Near the end of the risk assessment, Participant 1 noted that it had helped to have a structured method such as OCTAVE Allegro to use when considering vulnerabilities and threats. He stated that it created a more in-depth view of various issues, as it provided methodical steps with which to conduct risk identification. For instance, Participant 1 said that having the different Impact Areas (Worksheets 1-7) listed right in front of him was a good reminder to think through possible threats from areas that he had not previously considered. As an example, he mentioned "reputation" (Impact Area) as it related to GFU's Learning Management System (LMS).

The risk assessment process made Participant 1 realize that GFU IT staff needed to consider not only GFU's reputation external to their organization but also GFU's reputation among the GFU faculty. GFU's LMS was initially met with much faculty uncertainty, and faculty buy-in and adoption took a long time. If a student were able to breach the system and change student grades, this would significantly damage GFU's reputation in regard to the LMS, both externally and internally.

Further, Participant 1 said that, when he was going through Step 5, identifying threat scenarios by answering the questions found in the OCTAVE Allegro Questionnaires v1.0, he was made aware that he had been thinking only of threats that were possible by

exploiting technical containers, not threats caused by people. The questionnaires made the participant aware of vulnerabilities of IS assets through people and the processes that were used to access the asset. Participant 1 realized that GFU needs to address the risks that arise through people and processes involved in the information system.

Another example of the risk assessment participants' becoming aware of threats from non-technical containers was seen during the completion of Step 4. When brainstorming threat concerns in Step 4, GFU participants realized that certain departments most likely had paper copies of personal information of students that would be subject to Family Educational Rights and Privacy Act (FERPA) regulations. Other departments most likely had written medical information about students that would be subject to Health Insurance Portability and Accountability Act (HIPAA) regulations. The OCTAVE Allegro risk assessment made GFU participants aware of the vulnerabilities that exist through these physical containers (i.e., on paper).

After conducting some interviews and completing questionnaires from the OCTAVE Allegro Questionnaires v1.0, Participant 1 stated that, in working through Step 5 of OCTAVE Allegro (meant to help identify threat scenarios), he realized that there is an unspoken expectation in the GFU IT department that each person should keep security in mind as he or she is working in his or her own area. Participant 1 felt, however, that a very small percentage of the employees in their department actually considered security in their respective areas of responsibility. Using a structured method for risk assessment helped to highlight areas in need of being addressed.

Observations

Although GFU risk assessment participants felt that GFU IT staff members already had a fair understanding of the major threats and vulnerabilities of their most important IS assets, the author observed that, when working to complete the first part of the Information Asset Risk Worksheet (Worksheet 10), Participant 1 was looking at the OCTAVE Allegro Example Worksheets v1.0 to understand the fields such as Actor, Means, Motive, and Outcome for each identified threat. This exercise provided more detail about each threat than the GFU IT staff had previously considered.

Documentation

The final report produced as a result of the OCTAVE Allegro risk assessment consisted of the completed OCTAVE Allegro Worksheets. Normally there are multiple instances of the Information Asset Risk Worksheet (Worksheet 10) for each IS asset, as the risk assessment process requires participants to complete this worksheet for each threat scenario identified. Due to the constrained timeframe for the GFU risk assessment project, participants only completed Worksheet 10 for the one main threat scenario that they could easily identify for each of their IS assets; the participants did not complete the worksheet for all threat scenarios that were identified. However, in completing some of the OCTAVE Allegro Questionnaires v1.0, GFU participants identified numerous possible threat scenarios other than the ones of which they were previously aware. By going back to these questionnaires, GFU IT staff would be able to delineate other threats and risks that were previously overlooked.

Another valuable piece of information that was collected in the risk assessment process (and was included in the final OCTAVE Allegro report) was a qualitative

measure of the probability of a threat's being realized. Step 5 concerns the optional activity of assigning a perceived qualitative probability for the identified threat scenario. "Because it is often very difficult to accurately quantify probability (especially with respect to security vulnerabilities and events), probability is expressed in this risk assessment qualitatively as high, medium, or low" (Caralli et al., 2007, p. 52). GFU participants chose to add this optional probability to all identified threats, which was reflected in the final risk assessment report. Assigning a probability to each threat gave GFU one more measure by which to evaluate risks related to their IS assets.

For the analysis of the identified threats, Worksheet 10 also included a relative risk score, a quantitative value that represented the seriousness of the potential impact if the risk is realized. This relative risk score was derived from priorities that GFU identified earlier in the risk assessment process and provided a quantitative number by which to compare the impact of all identified risks. This quantitative number meant nothing by itself; it was meant only to provide a value with which to rate one risk against other identified risks. With the final OCTAVE Allegro risk assessment report, GFU obtained a more objective and quantitative measure by which to evaluate their security-related activities, rather than merely their intuition and experience, as was the case before the risk assessment project.

Results Related to RQ4

The fourth RQ is, To what extent will the completion of a risk assessment using the OCTAVE Allegro methodology provide adequate information for GFU IT staff to prioritize the security measures that should be employed to secure their IS assets? The results related to this question are presented in the material that follows.

The Baseline Situation

The final question to consider was the extent to which the completion of the OCTAVE Allegro risk assessment provided adequate information for GFU IT staff to prioritize the security measures that should be employed to secure their IS assets. At the start of the risk assessment project, GFU had no method for prioritizing security-related activities or an objective way to validate which security projects get funded. In an initial meeting with the author, the GFU IT contacts said that they did their security planning and operations intuitively, without confirmation by an objective method. In a formal interview before the risk assessment project, GFU participants verified this by indicating that security concerns were addressed as they arose within their environment, such as a denial-of-service attack on one of their network segments or servers.

As an example of how security-related priorities were set based on intuition and perceived cost, rather than following a structured method, the CFO commented on how GFU was checking into purchasing identity theft insurance to help transfer the risk of data breaches that might involve student data. GFU staff members were waiting to receive a quote for the cost of the insurance; the CFO said that knowing the cost could help in setting risk priorities. This belief was echoed by the outgoing CISO, who mentioned that he had a good idea about what the most important security-related issue might be, based on the expense of purchasing identity protection for all users if a data breach did occur. However, because the costs of all potential risks were not being considered, it would not be known whether there was a different risk that might have a greater impact on GFU.

Formal and Informal Interviews

When the risk assessment participants were asked whether they found the OCTAVE Allegro risk assessment useful to prioritize GFU security measures to secure their IS assets, Participant 1 said that it, indeed, was helpful. He specifically mentioned that setting a probability to the threats (in Step 5) helped give him a "three-dimensional view" of the threat scenarios; this substantially enhanced his understanding of the risks that were analyzed. Participant 1 mentioned that it would have been significantly more helpful if participants would have identified more threats and vulnerabilities for each asset but were unable to do so, based on time constraints for the risk assessment project.

During the final step of the OCTAVE Allegro risk assessment (Step 8, Select Mitigation Approach), Participant 1 created a relative risk matrix for the identified threats, which illustrated the importance of threats based on their relative risk score and the probabilities calculated in earlier steps. Participant 2 commented that it was nice to have this risk matrix to view and to compare IS risks in a way that GFU IT staff had not previously considered, rather than just repeating what the participants already knew from the outset of the risk assessment project.

Observations

Step 8 (Activity 1) of the OCTAVE Allegro risk assessment included instructions for the participant to prioritize the identified threats using a combination of their relative risk score and probability. The OCTAVE Allegro Method Guidance v1.0 provided an illustration of a Relative Risk Matrix as an example of using both risk score and probability to prioritize risks. On seeing this, Participant 1 was able to improvise and produce a prioritized view of threats in the matrix, using an element that showed GFU's

relative risk score on a linear scale within the matrix (Appendix G). This was an improvised view of GFU's identified risks; producing this chart showed that GFU is equipped with a risk-prioritization tool that GFU IT staff did not previously possess. GFU risk assessment participants were able to use this relative risk matrix to prioritize IS risks that had been identified and to decide whether to mitigate, defer, or accept the risk associated with each threat.

Documentation

The completed worksheets produced by participants of the OCTAVE Allegro risk assessment provided GFU with a detailed view of their IS assets and thorough documentation for each identified threat. The final steps in the risk assessment required that participants decide whether they would mitigate a particular risk, accept the risk, or defer the decision to mitigate. Decisions were made based predominantly on the relative risk matrix that the participants produced earlier. The risk matrix was able to provide GFU IT staff with the information that was needed to prioritize GFU's security-related activities, and GFU IT staff members now have a list of threats and decisions for handling the associated risks. The final activity for the OCTAVE Allegro risk assessment (Step 8, Activity 3) required the participants to detail the mitigation steps that IT staff would take for the risks that they decided to mitigate. This process provided GFU IT staff with a clear plan for employing certain security measures to protect their IS assets.

The GFU IT staff was already working on implementing mitigation solutions for some of the risks that were identified during the risk assessment process. This was due to the fact that, with their limited timeframe for the assessment, the participants listed only one

major threat scenario per IS asset, many of which GFU IT staff were already aware. However, the IT staff now has documentation that details the various aspects and consequences of these risks, a way to objectively prioritize these risks, and a tool to objectively justify which security projects are most important, which GFU IT staff previously did not have.

Summary

This chapter reported the results of the data as they related to each research question that formed the basis for this investigation. Data were collected by the author from different sources, including documentation, interviews, and observations. These multiple sources of data provided a convergence of evidence to answer the four research questions (Gillham, 2008; Yin, 2009). In summary, OCTAVE Allegro proved to be easy for GFU risk assessment participants to understand and conduct. Performing the risk assessment provided GFU IT staff with a more complete view of the details and security requirements of their IS assets. The process also helped GFU participants to identify threats and provided an objective method for prioritizing GFU IS security-related projects.

GFU IT staff previously planned their security-related measures and operations based on their intuition and experiences. GFU did not utilize a structured method to validate IS security concerns or an objective process to prioritize IS-related security projects. Although GFU performed an abridged version of the OCTAVE Allegro risk assessment based on a limited timeframe for completion, the process proved valuable for providing an objective view of GFU's risk environment and a repeatable process by which to evaluate security concerns and IT security projects. The GFU IT staff would like to build

OCTAVE Allegro risk assessment information into a regular part of their reporting process, as they see the importance of having a structured risk assessment process drive GFU's security decisions.

Chapter 5

Conclusions, Implications, Recommendations, and Summary

Introduction

This chapter presents the conclusions, implications, recommendations, and summary of this investigation. The chapter begins with the conclusions that were developed based on the results of this research, particularly as they pertain to the four research questions. This is followed by a presentation of the implications of the results in terms of their impact on the investigation of risk management and how it contributes to the professional practice of risk assessments in higher education. Then, recommendations for future research are provided, followed by a summary of this investigation.

As noted in the methodology section, throughout this research process, the author obtained input from experts in the implementation of OCTAVE Allegro and other risk assessment methods. Although all feedback received from these experts confirmed the results and conclusions of this investigation, the comments by Lisa Young, co-author of the OCTAVE Allegro methodology (Caralli et al., 2007), are especially worthy of note (Appendix H). Young confirmed that the findings of this report were valid in that they provided GFU with a more holistic view of risks to their IS assets. Young also stated that the findings of this investigation are generalizable to other small institutions of higher education.

Conclusions

As noted above, the research was structured around four research questions. The following conclusions are based on analysis of the case study results as they pertain to each research question.

Conclusions Related to RQ1

The first RQ is, To what extent is the OCTAVE Allegro methodology sufficiently straightforward for the IT staff at GFU to understand and conduct? Based on the results, it became evident that the OCTAVE Allegro method was easy for the GFU IT staff to understand and implement. The GFU participants had no previous knowledge of risk assessment methods and had never performed an IS risk assessment. Within a couple of hours, the GFU participants were able to read the pertinent parts of the OCTAVE Allegro Documentation (the appendices). With this degree of training and understanding, the participants were able to start completing the OCTAVE Allegro worksheets, which form the substance of the OCTAVE Allegro risk assessment method. GFU IT staff did not need formal training or supplemental written material to grasp the activities related to each step of the OCTAVE Allegro risk assessment process. Based on merely reading the documentation, the participants were able to complete a first iteration of the entire OCTAVE Allegro risk assessment within a couple weeks.

Conclusions Related to RQ2

The second RQ is, To what extent did conducting an OCTAVE Allegro risk assessment help GFU IT staff identify existing IS assets and classify them in order of importance to the mission of the organization? The OCTAVE Allegro risk assessment helped GFU to gain a more comprehensive view of their IS assets and to better

understand the security requirements associated with each asset. GFU had no centralized or formal written list of their IS assets. Although GFU IT staff were already aware of the university's important IS assets, the risk assessment process provided an opportunity to create formal documentation of their IS assets, including a description of each asset, why it was important to the university, and its data owner. Further, in talking to data owners to collect the information required by the OCTAVE Allegro Information Asset Profile, participants gained a better understanding of where the IS asset was stored and processed, how it was used by faculty and staff, and its security requirements.

Conclusions Related to RQ3

The third RQ is, To what extent did conducting an OCTAVE Allegro risk assessment help GFU IT staff identify and evaluate IS security concerns, including threats, vulnerabilities, and risks in regard to existing IS assets? Completing the OCTAVE Allegro risk assessment helped GFU IT staff to identify and evaluate security concerns. GFU had not previously used a method to identify security threats or to evaluate the IS risks to their university. The risk assessment participants were able to identify risk scenarios of which they were previously unaware. Further, the participants now have a more complete understanding of the risks that already had been identified. The process of recording the risks in the Information Asset Risk Worksheets helped the risk assessment participants to document the specific aspects of the threat, such as the means by which the threat could be carried out, the motive for the attack, and the extent of the impact if the threat were realized. Having a better understanding of the risk scenario details is beneficial to deciding how to mitigate the risk.

Completing the OCTAVE Allegro risk assessment also provided GFU with a quantitative relative risk score for each threat, which was calculated using the priorities that GFU had identified as business objectives important to their organization. Along with the risk score, OCTAVE Allegro also provided GFU with a qualitative probability score associated with each threat to help with risk evaluation and prioritization. Thus, GFU IT staff gained a more complete view of IS threats and has a method for evaluating these risks.

The extent to which the current iteration of the OCTAVE Allegro risk assessment provided GFU with valuable information, however, was limited, based on the restricted timeframe and resources that GFU IT staff were able to dedicate to the risk assessment project. Because GFU lost a couple of IT employees, they were forced to do an abridged version of the risk assessment. Because of the limited time that the participants spent on the risk scenario identification phase (Phase 3) of OCTAVE Allegro, the participants did not identify or document all the threat scenarios and risks that a complete risk assessment would have. OCTAVE Allegro did provide GFU with a process to identify further threats or an evaluation tool for risks. This will be more useful to GFU as IT staff members complete the rest of the Information Asset Risk Worksheets based on information regarding the risk assessment that participants have collected in the Threat Scenario Questionnaires (OCTAVE Allegro Questionnaires v1.0).

Conclusions Related to RQ4

The fourth RQ is, To what extent did the completion of the OCTAVE Allegro risk assessment provide adequate information that enabled GFU IT staff to prioritize the security measures that should be employed to secure their IS assets? Before completing

the OCTAVE Allegro risk assessment, the GFU IT department did not have a methodology for justifying to the management the necessity of GFU's IS security operations or a way to objectively set priorities for security-related plans and projects. The completion of this abridged OCTAVE Allegro risk assessment provided GFU with a relative risk matrix to view the risks to their IS assets and enabled GFU to prioritize security plans based on this objective view. The knowledge gained by the participants by conducting the OCTAVE Allegro risk assessment, along with the existence of the resulting relative risk matrix, provided GFU with an effective method to prioritize IS-related security measures.

Due to limited time spent on this iteration of the risk assessment project, however, a number of the risks listed in the OCTAVE Allegro worksheets were ones that already had been verbally identified by GFU IT staff and for which priorities previously had been decided. Although spending the time to put all threats into the risk matrix would produce more robust results, the results of this risk assessment project did provide a way for the IT department to justify to upper management the necessity of their current security priorities and projects. The view that GFU has of the risk to their IS assets will become more complete and will provide more useful prioritization insights as GFU IT staff spends time identifying and evaluating more threat scenarios. GFU would gain even more benefit if IT staff incorporated the OCTAVE Allegro risk assessment activities into a regular part of their IT responsibilities and include this risk information in management reporting, as the GFU IT staff is considering doing.

Implications

Impact on Risk Management Research

As noted by Bougaardt and Kyobe (2011) and Sanchez et al. (2010), there is a need for more research in the area of risk management for small- and medium-sized entities, such as post-secondary institutions. This investigation provides an important step in meeting the need for more research focused on IS risk assessments for small colleges and universities. This investigation offers an important finding in regard to risk assessments for small colleges and universities in that it has validated the feasibility of using OCTAVE Allegro in a small university environment and verified that a small university can obtain meaningful results from doing so.

The results of this investigation demonstrated that the OCTAVE Allegro methodology met the unique requirements of small- to medium-sized colleges and universities. These results are significant, as few other studies have validated the use of a particular risk assessment method in a small university environment (Al-Ahmad & Mohammad, 2013; Beranek, 2011; Sanchez et al., 2010). As described in the classic reports by Kvavik (2006) and Yanosky (2007), and then confirmed in recent reports by Grajek and Arroway (2012) and Keating (2012), fewer than half of all smaller institutions of higher education perform risk assessments of administrative systems. According to Sanchez et al. (2010), small- to medium-sized colleges and universities typically do not perform risk assessments due to a lack of financial resources or IT personnel with adequate computer security skills. Sanchez et al. also noted the need for the development of a risk assessment methodology that meets the specific requirements of smaller colleges and universities, specifically, a methodology that is easy to understand, provides detailed

worksheets, and is cost efficient. Identifying OCTAVE Allegro as an appropriate risk assessment method for small- and medium-sized institutions of higher education may help to remove an obstacle for many small colleges and universities as they struggle to find an appropriate risk assessment methodology for their environment.

Further, in recent literature, such as Al-Ahmad and Mohammad (2013) and Talabis and Martin (2013), there remains a misunderstanding of the feasibility of using OCTAVE Allegro to produce meaningful results in small- and medium-sized organizations. This investigation clearly sets OCTAVE Allegro apart from the two earlier versions of OCTAVE (the original OCTAVE Method and OCTAVE-S; Caralli et al., 2007) and demonstrates how it can be used successfully at a small university for conducting an effective risk assessment. Because the first two versions of OCTAVE were more difficult to use in terms of the amount of time and expertise required (Caralli et al., 2007; Talabis & Martin, 2013), it appears that OCTAVE Allegro is often grouped with these earlier variants and is, thus, characterized as too difficult to use in a smaller environment. According to Al-Ahmad and Mohammad, "Due to the level of activity and overhead involved in OCTAVE, it is probably best suited to large organizations or projects" (p. 34). Although Al-Ahmad and Mohammad correctly stated that there were three different models of OCTAVE, they failed to properly differentiate their requirements or characterize appropriate uses for each one (Caralli et al., 2007; Liu et al., 2009). Al-Ahmad and Mohammad provide a comparison table that characterizes OCTAVE Allegro as being inappropriate for small- and medium-sized organizations, needing outside consultation to complete, requiring a moderate level of skill, and having a medium cost of implementation. It appears that this characterization of OCTAVE Allegro was

incorrectly conceived, as that same table showed the original OCTAVE and OCTAVE-S to be low cost, appropriate for small- and medium-sized enterprises, and requiring only a simple skill level to complete, characteristics that should have instead been applied to OCTAVE Allegro (Caralli et al., 2007). Nevertheless, this apparent misunderstanding or misrepresentation is an example of what continues to appear in literature on OCTAVE Allegro.

Another example of the lack of a clear characterization of OCTAVE Allegro is found in Talabis and Martin (2013). Although Talabis and Martin did a good job of describing the OCTAVE Allegro process, they lumped it together with the earlier versions of OCTAVE and stated, "The detail level and complexity of the OCTAVE assessment approach has made it hard to adopt on a wide scale" (p. 29). Talabis and Martin also stated, "Even if Allegro is the streamlined version of OCTAVE, it is still relatively long and complex if followed to the letter when compared to other frameworks" (p. 34). However, the other frameworks compared in Talabis and Martin are the Factor Analysis of Information Risk (FAIR), NIST's *Guide for Conducting Risk Assessments*, and ISO/IEC 27005, which are known to be highly complex, require extensive resources to complete, and are not appropriate for smaller organizations (Beachboard et al., 2008; Sanchez et al., 2010).

Based on the results of this investigation that used OCTAVE Allegro, this author would challenge the idea that OCTAVE Allegro is difficult to understand or to use in completing a risk assessment, particularly when compared to other risk assessment methodologies or frameworks such as FAIR, COBIT, NIST, and ISO/IEC 27005. The author would encourage other studies to evaluate the ease of use and effectiveness of

OCTAVE Allegro in small- and medium-sized institutions of higher education and other organizations.

Contributions to Professional Practice

According to Sanchez et al. (2010), most of the widely accepted risk assessment frameworks and methods have been designed with larger organizations in mind. Previously, there have not been clearly identified risk assessment methods that will meet the unique needs of small- and medium-sized colleges and universities, which need a method that does not require a large outlay of finances or require highly experienced security personnel (Beachboard et al., 2008; Sanchez et al., 2010). The results of this investigation have shown that OCTAVE Allegro can provide meaningful risk assessment results while meeting the requirements of smaller universities. Thus, this investigation addressed an obstacle that has hindered IT personnel at smaller universities from completing a meaningful IS risk assessment.

This investigation has demonstrated that a meaningful IS risk assessment can be conducted by IT staff who are not security experts and who have had no previous training in risk management. OCTAVE Allegro provides a structured risk assessment methodology that is easy to understand, can be conducted in a relatively short timeframe, and can provide meaningful results. Even for a small IT department that is aware of their existing IS assets, performing an OCTAVE Allegro risk assessment provides a structured way to document what IS assets are important to the institution, to record their value to the institution, to explicitly record how they are used within the university, and to clearly identify their security requirements.

As presented in the results of this investigation, OCTAVE Allegro provides a cost-effective way for small universities to use a structured and repeatable method to identify and evaluate threats to their IS assets. The OCTAVE Allegro method gives small- and medium-sized colleges and universities access to an objective way to prioritize their security-related projects and plan for the most effective way to use limited resources to secure their IS assets.

Recommendations

Based on the findings from this investigation, the author recommends four areas for future research related to the topic of risk assessments in institutions of higher education. First, the author recommends that future research with the OCTAVE Allegro risk assessment include participants who receive more training than was done in this investigation. The OCTAVE Allegro Documentation indicates that the training requirements for successfully performing an OCTAVE Allegro risk assessment are minimal and that participants "should be able to use the guidance and worksheets included in this technical report without further instruction" (Caralli et al., 2007, p. 24). This case study at GFU took this approach; there was no training, except for participants' reading the specific guidance found in the appendices of the OCTAVE Allegro Documentation. The OCTAVE Allegro Documentation does suggest, however, that participants new to risk assessment should have some sort of training, even if it entails spending one or two days reading the entire OCTAVE Allegro Documentation found in Caralli et al. Further, SEI offers an official OCTAVE Training course (SEI Training, 2013), which the author attended prior to the start of this risk assessment project. This three-day course covers the entire OCTAVE Allegro risk assessment process and

includes lectures, in-class exercises that simulate performing a risk assessment, and discussions of the different OCTAVE Allegro activities. The author recommends that further research be performed whereby the risk assessment participants receive training from the official OCTAVE Training course (SEI Training, 2013) or an equivalent amount of training as part of a risk assessment project. It is anticipated that this additional training would improve the quality of the risk assessment conclusions and usefulness for risk prioritization.

Second, because GFU lost a couple of IT personnel at the start of this risk assessment investigation, GFU was forced to do an abridged version of the OCTAVE Allegro risk assessment. Based on this time constraint, the threat identification phase (Phase 3) was not completed in a manner that identified all security threat scenarios and, thus, provided limited benefit when analyzing and prioritizing risks (Phase 4). The author recommends that further investigation be done that would allow adequate time to thoroughly complete Phases 3 and 4. It is anticipated that there would be pronounced benefits from doing a more thorough threat identification and risk prioritization.

Third, IS security industry expert and co-author of the OCTAVE Allegro Documentation, Lisa Young, in an email to the author (Appendix F), stated, “the more that GFU can make the risk assessment a regular part of the management reporting . . . the better the continued identification and assessment of risk will be over time” (para. 4). This investigation was not longitudinal; it did not analyze the long-term benefits from continued use of OCTAVE Allegro, but such a study at a small- or medium-sized institution of higher education could be beneficial in providing insightful research. There would be benefit in knowing whether the long-term use of OCTAVE Allegro would

positively affect risk management at a small university in regard to such matters as the number and severity of security incidents, the ability to communicate the value of IS security projects to upper management, the development of risk priorities, and continued use of OCTAVE Allegro as beneficial in regular IT reporting.

Finally, this investigation focused on the use of OCTAVE Allegro at a small university. According to Keating (2012), 32% of the largest universities still do not perform risk assessments on their critical IS assets contained in administrative systems, as seen earlier in Table 1. Although OCTAVE Allegro is well suited to be used at smaller institutions, it was not designed to be limited to smaller-sized organizations (Caralli et al., 2007). The difficulty in using one of the more complex risk assessment frameworks may be a hindrance to the large universities that have not completed an IS risk assessment. The author recommends that future research validate the effective use of OCTAVE Allegro at a large university, the results of which could help to overcome further barriers to conducting a risk assessment by the large universities that do not currently utilize a risk assessment methodology.

Summary

This investigation focused on validating an IS risk assessment methodology for a small institution of higher education. Conducting a risk assessment is an important part of a comprehensive security management plan for any organization, including for colleges and universities (Kouns & Minoli, 2010; Landoll, 2011). The problem addressed in this investigation is the challenge for small colleges and universities of finding a risk assessment method that works in their environment. Many of the currently accepted risk assessment methodologies are designed for large organizations (Beranek,

2011; Sanchez et al., 2010). Small institutions of higher education often do not have the financial resources and security expertise to conduct these industry-accepted risk assessments (Beachboard et al., 2008; Sanchez et al., 2010). OCTAVE Allegro is a well-accepted risk assessment methodology (Liu et al., 2009) that has characteristics that make it ideal for use by smaller institutions (Caralli et al., 2007). The goal of this current research was to evaluate the effectiveness of OCTAVE Allegro at a small-sized university.

The research method chosen for this research was a single-case case study, which is appropriate when investigating a representative case and there is a need to capture the pertinent elements from the context of the organization (Yin, 2009). The case study was carried out at GFU in Newberg, Oregon, a small-sized university of approximately 3,500 FTE students (GFU, 2013a) and about 20 full-time IT staff members (GFU, 2013b). The unique study by Schuman (2005) included GFU as one of 12 institutions that represented a typical small-sized institution of higher education in the U.S.

There were four research questions addressed in this investigation, as follows.

RQ1. To what extent was the OCTAVE Allegro methodology sufficiently straightforward for the IT staff at GFU to understand and conduct?

RQ2. To what extent did conducting an OCTAVE Allegro risk assessment help GFU IT staff to identify existing IS assets and classify them in order of importance to the mission of the organization?

RQ3. To what extent did conducting an OCTAVE Allegro risk assessment help GFU IT staff to identify and evaluate IS security concerns, including threats, vulnerabilities, and risks in regard to existing IS assets?

RQ4. To what extent did the completion of a risk assessment using the OCTAVE Allegro methodology provide adequate information for GFU IT staff to prioritize the security measures that should be employed to secure their IS assets?

Right before the current risk assessment investigation began, GFU lost two of its top IT staff, the CIO and the Director of Administrative Computing (who also operated as CISO). This affected the ability of GFU to dedicate as much time and resources to the risk assessment project as had been previously planned. GFU IT staff were forced to do an abbreviated version of the OCTAVE Allegro method in that they identified only a representative number of threat scenarios in the threat identification phase (Phase 3) of the OCTAVE Allegro risk assessment.

According to Yin (2009), the preferred method to analyze case study evidence is to rely on the theoretical propositions that formed the basis of the investigation. Thus, the conclusions drawn from this investigation focus on addressing the four research questions that formed the basis of this research. Based on the outcomes of this investigation, the author concluded that the OCTAVE Allegro methodology was sufficiently straightforward for the IT staff at GFU to understand and conduct (RQ1). With no background in risk assessment, a network administrator from GFU's IT department was able to spend a couple hours reading the OCTAVE Allegro Documentation that was included in the appendices of Caralli et al. (2007) and to begin to conduct an OCTAVE Allegro risk assessment. The worksheets and guidelines contained in the OCTAVE Allegro Documentation provided clear guidance for completing the risk assessment. A review by risk assessment participants of the completed worksheets, provided as examples in the OCTAVE Allegro Documentation, clarified most participant questions.

Based on an examination of the outcomes of this investigation, the author determined that conducting the OCTAVE Allegro risk assessment significantly helped GFU IT staff to fully understand and document GFU's IS assets, such as ERP, LMS, and student financial data. During the process of the risk assessment, participants gained an increased understanding of who used the IS assets, why the assets were important to the university, who the owner of each asset was, and the assets' security requirements. In this sense, conducting the OCTAVE Allegro risk assessment helped GFU IT staff to identify existing IS assets and classify them in order of importance to the mission of the organization (RQ2). Although the GFU risk assessment participants were aware of GFU data assets and had a good feeling about which were most important, this information was not documented, nor was there a complete understanding of all the ways that data assets were used or their precise security requirements. Completing the OCTAVE Allegro risk assessment process provided GFU IT staff with a more comprehensive understanding of GFU IS assets.

Based on the outcomes of this investigation, the author further concluded that conducting the OCTAVE Allegro risk assessment helped GFU IT staff to identify and evaluate IS security concerns, including threats, vulnerabilities, and risks in regard to existing IS assets (RQ3). GFU risk assessment participants were able to identify and document threats of which they were unaware and were able to build a more complete picture of the threats about which they already knew. Completing the OCTAVE Allegro worksheets provided the risk assessment participants with a better understanding of specific aspects of each threat scenario, such as the means by which the threat could be carried out, the motive for the attack, and the extent of the impact if the threat were

realized. Completion of the OCTAVE Allegro risk assessment also provided GFU with a quantitative relative risk score for each threat, which was calculated based on organizational priorities and business drivers identified in Phase 1 of the OCTAVE Allegro risk assessment. Thus, GFU has a process by which to evaluate the IS security risks. Although the abridged nature of the risk assessment at GFU allowed for only a limited number of threat scenarios to be identified, OCTAVE Allegro provided GFU with a systematic process to identify further threats and prioritize IS security risks.

Finally, based on the outcomes of this investigation, the author concluded that the completion of the OCTAVE Allegro risk assessment provided adequate information for GFU IT staff to prioritize the security measures that should be employed to secure their IS assets (RQ4). Not having a way to objectively prioritize IS risk was one of GFU IT staff's original concerns. Using the OCTAVE Allegro risk assessment provided GFU with a structured and repeatable method for prioritizing more risks as they are identified. Whereas the IT staff previously had no way of objectively justifying their IS security operations and projects, the OCTAVE Allegro risk assessment produced a relative risk matrix by which to view all identified risks and prioritize them according to the business drivers of the university. The results helped to validate some of the priorities of GFU's current security projects, which had been based on GFU IT staff intuition. However, the benefits of prioritizing GFU IS risks were limited based on the abridged version of the threat identification phase and, thus, provided only a small number of identified risks in the relative risk matrix.

Importantly, this research has implications for risk assessments at small colleges and universities. This investigation identified and validated OCTAVE Allegro as a risk

assessment methodology that is appropriate for use at such institutions. According to Sanchez et al. (2010), small- to medium-sized institutions of higher education often do not perform risk assessments because of lack of financial resources and IT personnel who lack adequate IS security experience. Sanchez et al. also highlighted the need for the development of a risk assessment methodology that would meet the specific requirements of smaller organizations, such as the methodology's being simple and cost efficient. The identification and validation of OCTAVE Allegro as a risk assessment method that meets the needs of small universities may encourage more small colleges and universities to take on the important task of performing an IS risk assessment.

Based on the findings from this investigation, the author identified four recommendations for future research. First, the GFU risk assessment participants had minimal training before completing the OCTAVE Allegro risk assessment project. The author recommends that further research be conducted that would include the risk assessment participants' attending the official SEI OCTAVE Training course (SEI Training, 2013) before conducting the risk assessment. Second, GFU risk assessment participants performed an abridged version of the threat identification phase (Phase 3) of OCTAVE Allegro, which limited the value of the risk assessment results. The author recommends that future research include a study whereby the participants take the time needed to thoroughly complete the threat identification phase. Third, the author recommends a longitudinal study be conducted to investigate the benefits of using OCTAVE Allegro as part of continued management reporting, as the author anticipates that this would improve the identification and assessment of risk for the university. Fourth, this investigation was done at a small university. The author recommends that

future research should study the effectiveness of OCTAVE Allegro at a large university, as 32% of large-sized universities do not perform regular IS risk assessments on administrative systems (Keating, 2012).

Appendix A

GFU Consent to Participate in Research

E-mail from Greg Smith Confirming GFU as Location for Risk Assessment

From: Greg Smith
Sent: Thursday, December 17, 2009 1:07 PM
To: Corland Keating
Subject: Re: PhD Dissertation Research at GFU

I would like to confirm that George Fox University is looking forward to working with Corland on an OCTAVE Allegro risk assessment for various data sets at our university. This is the type of project that we have wanted to perform, but making it happen in the typical hectic IT schedule is a challenge. We have a fairly solid security and sys admin focus here at GFU but no experience with this specific risk assessment. My newly identified Chief Security Officer, Sean McKay, will also be actively involved.
--
Greg Smith
Chief Information Officer
George Fox University

Appendix B

Acronyms

CCTA	Central Computer and Telecommunications Agency
CFO	Chief Financial Officer
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CMU	Carnegie Mellon University
COBIT	Control Objectives for Information and related Technology
CRAMM	CCTA Risk Analysis and Management Method
PCI DSS	Payment Card Industry Data Security Standard
ECAR	EDUCAUSE Center for Applied Research
ERA Utility	Digital Defense Inc.'s Enterprise Risk Assessment Utility
ERP	Enterprise Resource Planning
FAIR	Factor Analysis of Information Risk
FERPA	Family Educational Rights and Privacy Act
FISMA	Federal Information Security Management Act
FRAAP	Facilitated Risk Analysis and Assessment Process
FTE	Full-time equivalent
GFU	George Fox University
HIPAA	Health Insurance Portability and Accountability Act
IP	Internet Protocol
IS	Information Systems
ISO/IEC	International Organization for Standardization/International Electrotechnical Commission

IT	Information Technology
LMS	Learning Management System
NIST	National Institute of Standards and Technology
OCTAVE	Operationally Critical Threat, Asset, and Vulnerability Evaluation
RQ	Research Question
SEI	Carnegie Mellon University's Software Engineering Institute
SP	Special Publication (by NIST)

Appendix C

Pre-Risk Assessment Structured Interview Questions

1) Does GFU have IT staff dedicated to IS security?
   a) If not, who has the responsibility of addressing the IS security concerns at GFU?

2) What is the process for updating GFU's security policies and procedures?

3) Has GFU conducted an IS risk assessment in the past?
   a) If so, how often does GFU do so?
   b) If so, on which assets were the assessment performed (e.g., IT systems/ infrastructure, central administrative systems/data)?
   c) If GFU has conducted a risk assessment in the past, what has been the outcome or benefits received?

4) What is the process for determining which security projects get funded? Or how are security concerns prioritized?

5) Does GFU maintain a list of all IS assets, including all data? What is the process of prioritizing them in terms of importance to the mission of GFU?

6) Does GFU maintain documentation as to what systems store and transport which data assets?

7) Does GFU perform vulnerability analysis/scans on IT assets?
   a) If so, what methods or tools are used to do so?
   b) If so, who carries out these scans?

8) You mentioned in our initial meeting that you believe you know intuitively where your greatest risk currently lies and the area you would want to do a more formal risk assessment on (based on the expense of purchasing identity protection for all users). What area is that?

9) How does GFU record detected security breaches and incidents?
   a) What kind of action was taken for these past incidents?
   b) What process is in place for handling incidents?

10) Does GFU regularly perform penetration testing or vulnerability scans on their IS assets, or perform other actions to capture vulnerabilities (or do threat analysis)? What happens with the outcomes of these activities?

11) What is GFU's process for calculating IS asset vulnerability and risk?

Appendix D

Post-Risk Assessment Structured Interview Questions

1) How straightforward did you find the OCTAVE Allegro methodology to be? (Is it understandable? Do you think more training would have benefited you? Any parts you found difficult to understand?)

2) How useful did you find the OCTAVE Allegro risk assessment to be for identifying existing IS assets? (Did it give you a better picture of your assets? What about identifying the data owners, or containers, or how they are used?)

3) How useful did you find the OCTAVE Allegro risk assessment to be for classifying IS assets or rating them in terms of their order of importance to the mission of GFU? (Did it highlight or give you insight into their values? Did it change your thinking about the importance of any of the assets [either elevating them or lowering them]?

4) How useful did you find the OCTAVE Allegro risk assessment to be for identifying and evaluating IS security concerns, including threats, vulnerabilities, and risks in regard to existing IS assets? (Did it help you identify vulnerabilities or threats that you were not previously aware of? Did it help give you a better evaluation of the risks to your assets? Do you think you have a better understanding of the risks to your IS assets?)

5) How useful did you find the OCTAVE Allegro risk assessment to be for providing information for IT staff to prioritize the security measures that should be employed to secure their IS assets? (Do you have a better understanding of what areas need to be worked on to secure? Did this change from when you started the risk assessment? [If did not change in that the top ones are the same,] after working on the top couple concerns, do you have a better feel for other security measures that need to be employed that you were not aware of previously?)

6) Do you have any other comments about the OCTAVE Allegro risk assessment process at GFU that you would like to share?

Appendix E

Risk Assessment Professionals' Consent to Participate in Research

E-mail from Lisa Young Confirming Feedback for Risk Assessment

From: Lisa R. Young
Sent: Thursday, December 03, 2009 11:02 AM
To: Corland Keating
Subject: RE: OCTAVE Allegro Research in Higher Ed
Attachments: example metrics for the RMM risk management process.docx

Corland,

I would be happy to help. I have attached a list of process metrics I am using in some of my current Resiliency Management Model (RMM) Risk Management work. If they fit into your research you are welcome to use them to validate your results. For example, if someone institutionalized the Allegro method as a part of regular management activities, would these be the metrics that would give them an indication of their risk management capabilities? Check out www.cert.org/resiliency for more info on RMM.

Regards, Lisa

E-mail from Steffani Burd Confirming Feedback for Risk Assessment

From: Steffani Burd, Ph.D.
Sent: Monday, December 07, 2009 6:06 AM
To: Corland Keating
Subject: RE: An Update: OCTAVE Allegro Research in Higher Ed

Dear Corland,

I would be delighted to help you. Am comfortable with the areas you listed as needing input and look forward to being a resource for you - and congratulations on your continued progress! Feel free to let your advisor know that I'm delighted to help you with this process.

Kind regards and congratulations again on your ongoing progress!

Steffani

Email from Kathleen Roberts Confirming Feedback for Risk Assessment

From: Kathleen Roberts
Sent: Friday, March 19, 2010 8:19 AM
To: 'Corland Keating'
Subject: RE: A Question - OCTAVE Allegro Research in Higher Ed

Corland,

Received your email and apologize for the much delayed response. 4Q09 and 1Q10 have been tough both professionally and personally.

All that to say that I am still interested and willing to assist your efforts! Please provide a status of your Idea Paper, an update on your research design method and let me know what your dissertation timeline looks like.

Look forward to working together.

Take care,
Kathleen

_____

Kathleen K. Roberts
Founder and Principal
www.isecuresolutions.com

Appendix F

Professional Input before Risk Assessment Project

From: Lisa R. Young
Sent: Tuesday, November 20, 2012 10:03 AM
To: Corland Keating
Subject: RE: OCTAVE Allegro Research in Higher Ed—Dissertation Proposal Approved

Corland,

Congrats on making progress on your dissertation. I have read the methodology and it follows the constructs laid out for conducting an OCTAVE assessment.

There are a couple of things that may be useful to know about doing an assessment in the field. First, the risk measurement criteria are often the hardest to formulate, even for organizations that are experienced in risk management. Also, from a risk response perspective, the more you can make the criteria quantitative rather than qualitative, the better you are able to prioritize the identified risks. For example, try to put thresholds on the qualitative criteria like this for Reputation: GFU shows up in the local newspaper in an unfavorable light one time in a year—Low; GFU shows up in the local newspaper 6 times annually in an unfavorable light—Moderate; GFU shows up in the local paper and the national news story one time annually in an unfavorable light—High.

You should work with GFU to establish what they believe are their tolerances in each of the categories. One other category that we have added for institutions of higher learning is the category of "Teaching time." If there were a risk that was realized and it meant that the campus facilities or distance learning was not available for X time period, it would result in Y impact. Find out what the range of unavailability is for those types of risks at GFU and what types of risk could cause that to happen.

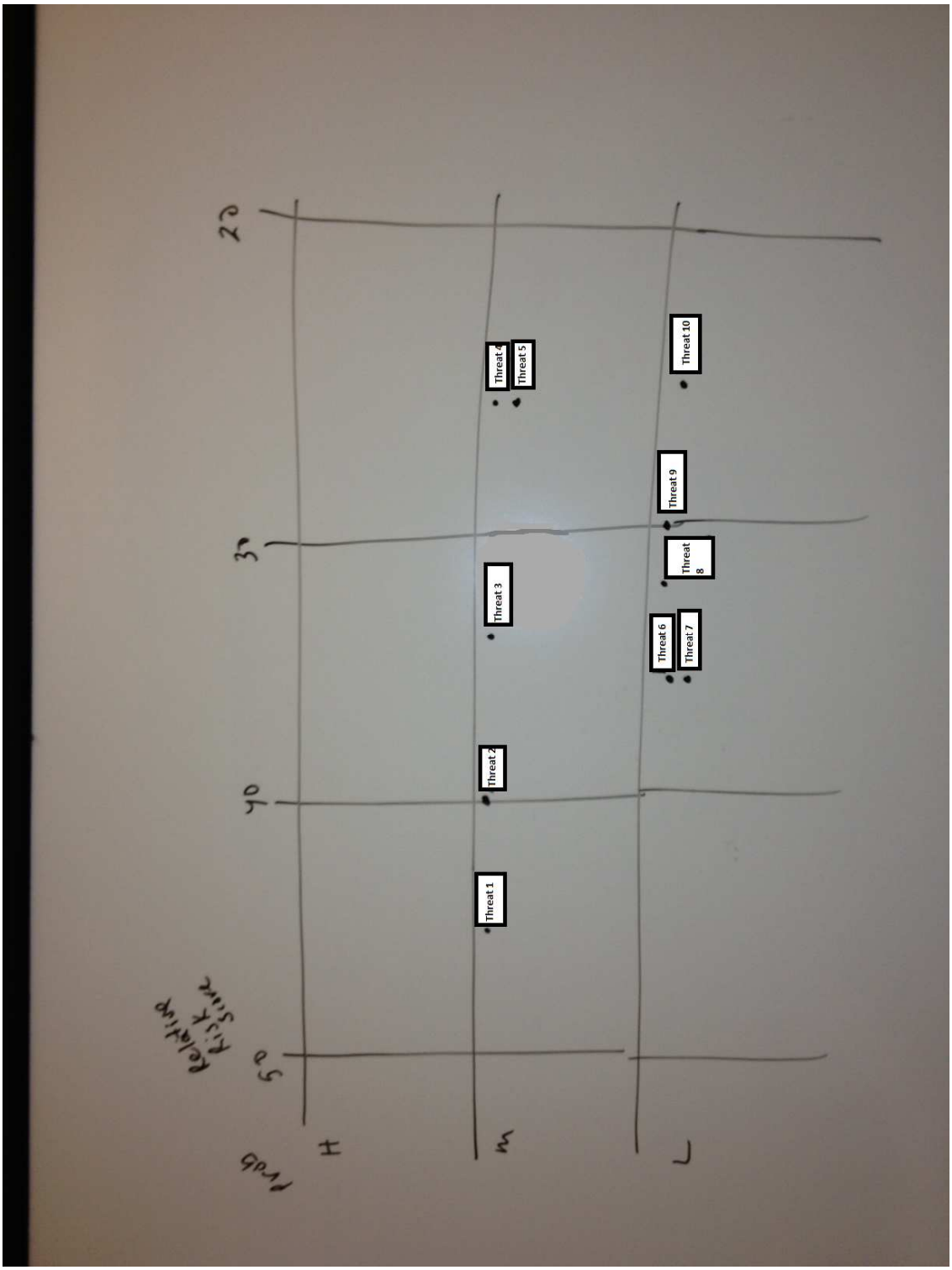
Second, the more that GFU can make the risk assessment a regular part of the management reporting, perhaps by leveraging any compliance reporting that management has to provide on a regular basis, the better the continued identification and assessment of risk will be over time.

I wish you the best.

Lisa

Appendix G

Improvised Relative Risk Matrix



Appendix H

Professional Input after Review of Results and Conclusions

From: Lisa R. Young
Sent: Monday, September 02, 2013 7:34 AM
To: Corland Keating
Subject: RE: Final Input for My Dissertation!

Corland,

Well done! I read the Introduction, Chapter 4, Chapter 5, and skimmed through the rest of the paper, including the appendices. I was glad to see that the folks at GFU were able to use the method by reading the workbook materials. One of the goals of Allegro was to make it simple to use but still provide good value for the organization. To answer your questions:

1. Your findings are valid in that they provide GFU a way to more completely and holistically understand risks to the organization, not just technology risks. I was particularly glad to see that Participant 1 came to the conclusion that people and process are important also. So, yes, the findings are valid.

2. Yes, the findings are generalizable to other small universities. I have used the Allegro method to assist other small organizations and often the most useful outcome is the awareness that comes from understanding how important the underlying assets are to the mission of the organization. All organizations, particularly small organizations, need to understand that service/mission delivery depends on assets.

I do think the implications are right on and the Allegro method does get conflated with the other OCTAVE methods.

Thank you again for letting me be a part of your journey.
Regards, Lisa

From: Corland Keating
Sent: Saturday, August 31, 2013 5:37 PM
To: Lisa R. Young
Subject: FW: Final Input for My Dissertation!
…
The two questions that I really need input on are:
1) If my findings are valid (as a risk assessment), and
2) If the OCTAVE Allegro method (according to the results I found at GFU) would be applicable to (generalizable to/useful at) other small universities.

Reference List

Agee, A. S., & Yang, C. (2009). Top-ten IT issues, 2009. *EDUCAUSE Review, 44*(4), 45-58.

Al-Ahmad, W., & Mohammad, B. (2013). Addressing information security risks by adopting standards. *International Journal of Information Security Science*, *2*(2), 28-43.

Alberts, C., & Dorofee, A. (2003). *Managing information security risks: The OCTAVE approach*. Boston, MA: Addison-Wesley.

Alberts, C., Dorofee, A., Stevens, J., & Woody, C. (2005). *OCTAVE-S implementation guide, version 1.0* (No. CMU/SEI-2003-HB-003). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University.

Alberts, C. J., Behrens, S. G., Pethia, R. D., & Wilson, W. R. (1999). *Operationally critical threat, asset, and vulnerability evaluation (OCTAVE) framework, 1.0* (No. CMU/SEI- 99-TR-017, ESC-TR-99-017). Pittsburgh, PA: Software Engineering Institute: Carnegie Mellon University.

Allen, J. H. (2013). Risk-centered practices. *Build security in.* Retrieved from https://buildsecurityin.us-cert.gov/articles/best-practices/deployment-and-operations/risk-centered-practices

Appari, A., & Johnson, M. E. (2010). Information security and privacy in healthcare: Current state of research. *International Journal of Internet and Enterprise Management, 6*(4), 279-314.

Beachboard, J., Cole, A., Mellor, M., Hernandez, S., Aytes, K., & Massad, N. (2008). Improving information security risk analysis practices for small- and medium-sized enterprises: A research agenda. *Issues in Informing Science and Information Technology, 5,* 73-85.

Beranek, L. (2011). Risk analysis methodology used by several small and medium enterprises in the Czech Republic. *Information Management & Computer Security, 19*(1), 42-52.

Blustain, H., Abraham, J. M., Adair, R. L., Carmichael, E. J., Klinksiek, G., & Thompson, J. W. (in press). Risk management. *College and University Business Administration. National Association of Colleges and University Business Officers (NACUBO).* Retrieved from http://www.nacubo.org/Products/Online_Publications/CUBA_7.html

Blustain, H., Chinniah, N., Newcomb, S., Plympton, M., & Walsh, J. (in press). Information technology and services. *College and University Business Administration.*

National Association of Colleges and University Business Officers (NACUBO). Retrieved from http://www.nacubo.org/Products/Online_Publications/CUBA_7.html

Bougaardt, G., & Kyobe, M. (2011). Investigating the factors inhibiting SMEs from recognizing and measuring losses from cyber crime in South Africa. *The Electronic Journal Information Systems Evaluation, 14*(2), 167-178.

Bruijn, W. D., Spruit, M. R., & van den Heuvel, M. (2010). Identifying the cost of security. *Journal of Information Assurance and Security*, *5*, 74-83.

Burd, S. A. (2006). *The impact of information security in academic institutions on public safety and security: Assessing the issues and developing solutions for policy and practice* (National Criminal Justice Publication No. 215953). Retrieved from http://www.ncjrs.gov/App/Publications/abstract.aspx?ID=237542

Caralli, R. A., Stevens, J. F., Young, L. R., & Wilson, W. R. (2007). *Introducing OCTAVE Allegro: Improving the information security risk assessment process* (No. CMU/SEI-2007-TR-012, ESC-TR-2007-012). Pittsburgh, PA: Software Engineering Institute: Carnegie Mellon University.

Carnegie Foundation for the Advancement of Teaching. (2010). *Summary tables: Size and setting classification.* Retrieved from http://classifications.carnegiefoundation.org/summary/size_setting.php

Collins, J. D., Sainato, V. A., & Khey, D. N. (2011). Organizational data breaches 2005-2010: Applying SCP to the healthcare and education sectors. *International Journal of Cyber Criminology, 5*(1), 794–810.

Cone, J. D., & Foster, S. L. (2006). *Dissertations and theses from start to finish: Psychology and related fields* (2nd ed.). Washington, DC: American Psychological Association.

Creswell, J. W. (2003). *Research design: Qualitative, quantitative, and mixed methods approaches* (2nd ed.). Thousand Oaks, CA: Sage.

Creswell, J. W. (2007). *Qualitative inquiry & research design: Choosing among five approaches* (2nd ed.). Thousand Oaks, CA: Sage.

Culnan, M. J., & Carlin, T. J. (2009). Online privacy practices in higher education: Making the grade? *Communications of the ACM, 52*(3), 126-130.

Curtis, P. D. (2009, August 19). OCTAVE Allegro speeds up the risk assessment process. *News at SEI*. Retrieved from http://www.sei.cmu.edu/library/abstracts/news-at-sei/01feature200705.cfm

Darke, P., Shanks, G., & Broadbent, M. (1998). Successfully completing case study research: Combining rigour, relevance and pragmatism. *Information Systems Journal, 8*(4), 273-289.

DeSot, T. (2008). Reader technology questions. *Credit Union Journal, 12*(43), 22.

Dhillon, G., & Torkzadeh, G. (2006). Value-focused assessment of information system security in organizations. *Information Systems Journal, 16*(3), 293-314.

Digital Defense Inc. (2009). *Digital defense announces major service launch with SEI OCTAVE Allegro compliant management tool.* Retrieved from http://www.ddifrontline.com/pdf/pr20080303.pdf

Dodge, A. (2009). Educational security incidents (ESI) year in review-2008. *Educational Security Incidents (ESI).* Retrieved from http://www.adamdodge.com/esi/files/esi_yir_2008.pdf

EDUCAUSE/Internet2 Computer and Network Security Task Force. (2008). *Security task force 2008-2009 strategic plan: Safeguarding our IT assets, protecting our community's privacy* (ID: CSD5494). Retrieved from http://net.educause.edu/ir/library/pdf/CSD5494.pdf

EDUCAUSE/Internet2 Computer and Higher Education Information Security Council. (2013). *Risk management framework, version 2.0.* Retrieved from https://wiki.internet2.edu/confluence/display/itsg2/Risk+Management+Framework

Ekelhart, A., Fenz, S., & Neubauer, T. (2009). *AURUM: A framework for information security risk management.* Paper presented at the 42nd Hawaii International Conference on System Sciences, Waikoloa, Big Island, Hawaii.

European Network and Information Security Agency (ENISA). (2010). *ENISA emerging and future risks framework: Introductory manual.* Retrieved from http://www.enisa.europa.eu/act/rm/emerging-and-future-risk/deliverables/emerging-and-future-risks-framework-introductory-manual

Ewell, C. V. (2009, June). A method[ology] to the madness. *Information Security Magazine,* 21-29.

Fenz, S., & Ekelhart, A. (2011). Verification, validation, and evaluation in information security risk management. *IEEE Security & Privacy, 9*(2), 58-65.

George Fox University (GFU). (2013a). *About our Christian university.* Retrieved from http://www.georgefox.edu/about/index.html

George Fox University (GFU). (2013b). *IT staff.* Retrieved from http://www.georgefox.edu/offices/it/about-it/it-staff.html

Ghernaouti-Helie, S., Simms, D., & Tashi, I. (2009, August). *Reasonable security by effective risk management practices: From theory to practice.* Paper presented at the International Conference on Network-Based Information Systems, Indianapolis, IN.

Ghernaouti-Helie, S., Tashi, I., & Simms, D. (2011, March). *Optimizing security efficiency through effective risk management.* Paper presented at the International Conference on Advanced Information Networking and Applications Workshops, Biopolis, Singapore.

Gillham, B. (2008). *Case study research methods*. London, UK: Continuum. (Original work published 2000)

Grajek, S. (2013). Top-ten IT issues, 2013: Welcome to the connected age. *EDUCAUSE Review, 48*(3), 30-57.

Grajek, S., & Arroway, P. (2012). *The EDUCAUSE 2011 core data service report: Highlights and insights into higher education information technology.* Retrieved from http://net.educause.edu/ir/library/pdf/PUB8008.pdf

Groner, R., & Brune, P. (2012). Towards an empirical examination of IT security infrastructures in SME. In A. Jøsang & B. Carlsson (Eds.), *Secure IT Systems* (Vol. 7617, pp. 73-88), Berlin, Germany: Springer.

Haller, J., Merrell, S., Butkovic, M., & Wilke, B. (2011). Best practices for national cyber security: Building a national computer security incident management capability. *CERT Program, Technical Report CMU/SEI-2011-TR-015.* Retrieved from http://www.sei.cmu.edu/reports/11tr015.pdf

Hedrick, G., & Grama, J. (2013). Information security. *EDUCAUSE Center for Applied Research*. Retrieved from http://www.educause.edu/library/resources/information-security-1

Holgate, J., Williams, S. P., & Hardy, C. A. (2012). Information security governance: Investigating diversity in critical infrastructure organizations. *Proceedings of the 2012 Bled eConference.* Retrieved from http://aisel.aisnet.org/bled2012/13/

Identity Theft Resource Center (ITRC). (2011). *2010 ITRC breach Stats.* Retrieved from http://www.idtheftcenter.org/artman2/uploads/1/ITRC_Breach_Stats_Report_20101229.pdf

Identity Theft Resource Center (ITRC). (2012). *2011 ITRC breach stats.* Retrieved from http://www.idtheftcenter.org/artman2/uploads/1/ITRC_Breach_Stats_Report_2011_20120207.pdf

Ingerman, B. L., & Yang, C. (2010). Top-ten IT issues, 2010. *EDUCAUSE Review, 45*(3), 46-60.

Ingerman, B. L., & Yang, C. (2011). Top-ten IT issues, 2011. *EDUCAUSE Review, 46*(3), 24-40.

International Organization for Standardization/International Electrotechnical Commission (ISO/IEC). (2008). *Information technology—Security techniques—Information security risk management* (Vol. ISO/IEC 27005). Geneva, Switzerland: Author.

Jenkins, R. (2009, December). *IT audit and risk assessment: Protecting customer information* (Version 64). Retrieved from http://knol.google.com/k/it-audit-and-risk-assessment

Johnson, E. M., Goetz, E., & Pfleeger, S. L. (2009). Security through information risk management. *IEEE Security and Privacy, 7*(3), 45-52.

Jones, M. (2009). An evaluation of privacy and security issues at a small university. *The Technology Interface Journal, 10*(2). Retrieved from http://technologyinterface.nmsu.edu/Winter09/Winter09/jones.pdf

Keating, C. (2012). Information systems risk assessment. *EDUCAUSE Center for Applied Research.* Retrieved from http://www.educause.edu/library/resources/information-systems-risk-assessment

Kouns, J., & Minoli, D. (2010). *Information technology risk management in enterprise environments: A review of industry practices and a practical guide to risk management teams*. Hoboken, NJ: John Wiley & Sons.

Kvavik, R. B. (with Voloudakis, J.) (2006). *Safeguarding the tower: IT security in higher education 2006* (Vol. 6, p. 132). Boulder, CO: EDUCAUSE Center for Applied Research.

Landoll, D. (2011). *The security risk assessment handbook: A complete guide for performing security risk assessments* (2nd ed.). Boca Raton, FL: CRC Press.

Lang, L., Grama, J., Norin, M., & Workman, S. (2013) Core data service 2013: Core metrics on IT financials, staffing, and services. *EDUCAUSE.* Retrieved from http://www.educause.edu/sites/default/files/library/presentations/E13/SESS133/CDSResults_131010.pptx_.pdf

Leeden, K. (2010). *Security without risk? Investigating information security among Dutch universities* (Master's thesis, University of Twente, Enschede, The Netherlands). Retrieved from http://purl.utwente.nl/essays/60026

Levy, Y., & Ellis, T. J. (2006). A systems approach to conduct an effective literature review in support of information systems research. *Informing Science, 9,* 181-212.

Liu, S., Kuhn, R., & Rossman, H. (2009). Understanding insecure IT: Practical risk assessment. *IT Professional, 11*(3), 57-59.

Luesebrink, M. J. (2011). *The institutionalization of information security governance structures in academic institutions: A case study* (Unpublished doctoral dissertation, Florida State University, Tallahassee, FL). Retrieved from http://etd.lib.fsu.edu/theses/available/etd-07272011-164711/

Marks, A., & Rezgui, Y. (2009, September 20-22). *A comparative study of information security awareness in higher education based on the concept of design theorizing.* Paper presented at the International Conference on Management and Service Science, Wuhan, China.

McCallister, E., Grance, T., & Scarfone, K. (2009). *Guide to protecting the confidentiality of personally identifiable information (PII)* (Special Publication 800-122 Draft). Gaithersburg, MD: National Institute of Standards and Technology.

McCumber, J. (2005). *Assessing and managing security risk in IT systems: A structured methodology.* Boca Raton, FL: Auerbach.

National Counterintelligence Policy Board. (2009). *The national counterintelligence strategy of the United States of America*. Retrieved from http://www.ncix.gov/publications/strategy/docs/NatlCIStrategy2009.pdf

Nikolic, B., & Ruzic-Dimitrijevic, L. (2009). Risk assessment of information technology systems. *Issues in Informing Science and Information Technology, 6*, 595-615.

National Institute of Standards and Technology (NIST). (2013). *National initiative for cybersecurity education (NICE).* Retrieved from http://csrc.nist.gov/nice/

NIST Joint Task Force Transformation Initiative. (2012). *Guide for conducting risk assessments: Recommendations of the National Institute of Standards and Technology* (Vol. NIST Special Publication 800-30 Rev. 1). Gaithersburg, MD: National Institute of Standards and Technology (NIST).

NIST Joint Task Force Transformation Initiative. (2011). *Managing information security risk: organization, mission, and information system view: Recommendations of the National Institute of Standards and Technology* (Vol. NIST Special Publication 800-39). Gaithersburg, MD: National Institute of Standards and Technology (NIST).

NIST Joint Task Force Transformation Initiative. (2013). *Recommended security controls for federal information systems and organizations: Recommendations of the National Institute of Standards and Technology* (Vol. NIST Special Publication 800-53 Rev. 4). Gaithersburg, MD: National Institute of Standards and Technology (NIST).

Peltier, T. R. (2010). *Information security risk analysis* (3rd ed.). Boca Raton, FL: Auerbach.

Ponnam, A., Harrison, B., & Watson, E. (2009). Information systems risk management: An audit and control approach. In J. N. D. Gupta & S. K. Sharma (Eds.), *Handbook of research on information security and assurance* (pp. 68-84). Hershey, PA: Information Science Reference.

Sanchez, L. E., Ruiz, C., Fernandez-Medina, E., & Piattini, M. (2010, February). *Managing the asset risk of SMEs.* Paper presented at the 2010 International Conference on Availability, Reliability, and Security, Krakow, Poland.

Schuman, S. (2005). *Old main: Small colleges in twenty-first century America*. Baltimore, MD: The Johns Hopkins University Press.

SEI Training. (2013). *Assessing information security risk using the OCTAVE approach.* Retrieved from http://www.sei.cmu.edu/training/p10b.cfm

Sekaran, U., & Bougie, R. (2009). *Research methods for business: A skill building approach* (5th ed.). Hoboken, NJ: John Wiley & Sons.

Smith, S. D., & Caruso, J. B. (2010). *The ECAR study of undergraduate students and information technology, 2010.* Boulder, CO: EDUCAUSE Center for Applied Research.

Syalim, A., Hori, Y., & Sakurai, K. (2009, March). *Comparison of risk analysis methods: Mehari, Magerit, NIST800-30 and Microsoft's Security Management Guide*. Paper presented at the 2009 International Conference on Availability, Reliability and Security, Fukuoka, Japan.

Talabis, M., & Martin, J. (2013). *Information security risk assessment toolkit: Practical assessments through data collection and data analysis*. Waltham, MA: Syngress.

Talbot, J., & Jakeman, M. (2009). *Security risk management body of knowledge* (2nd ed.). Hoboken, NJ: Wiley.

Tohidi, H. (2011). The role of risk management in IT systems of organizations. *Procedia Computer Science, 3,* 881-887.

Voloudakis, J. (2006). The continuing evolution of effective IT security practices. *EDUCAUSE Review, 41*(5), 30-44.

Whitman, M. E., & Mattord, H. J. (2010). *Management of information security* (3rd ed.). Boston, MA: Course Technology.

Widup, S. (2010). The leaking vault: Five years of data breaches. Retrieved from http://www.digitalforensicsassociation.org/storage/The_Leaking_Vault-Five_Years_of_Data_Breaches.pdf

Woody, C. C. (with J. Coleman, M. Fancher, C. Myers, & L. Young). (2006). *Applying OCTAVE: Practitioner's report.* (No. CMU/SEI-2006-TN-010). Pittsburgh, PA: Software Engineering Institute: Carnegie Mellon University.

Yanosky, R. (2007). *Shelter from the storm: IT and business continuity in higher education*. Boulder, CO: EDUCAUSE Center for Applied Research.

Yanosky, R. (2009). *Institutional data management in higher education*. Boulder, CO: EDUCAUSE Center for Applied Research.

Yin, R. K. (2009). *Case study research: Design and methods* (4th ed.). Thousand Oaks, CA: Sage.

Young, L., & Allen, J. (2008). Security risk assessment Using OCTAVE Allegro [Podcast]. *CERT's Podcast Series.* Retrieved from http://www.cert.org/podcast/show/20080916young.html

Young, M. (2010). *Study of cyber security professionals in the academic domain* (Unpublished Master's thesis). Pennsylvania State University, University Park, PA.

The Graduate School of Computer and Information Sciences

Certification of Authorship of Dissertation Work

Submitted to Advisor: Dr. Marlyn Kemper Littman

Student's Name: Corland G. Keating

Date of Submission: January 14, 2014

Purpose and Title of Submission: Dissertation Report: Validating the OCTAVE Allegro Information Systems Risk Assessment Methodology: A Case Study

Certification of Authorship: I hereby certify that I am the author of this document and that any assistance I received in its preparation is fully acknowledged and disclosed in the document. I have also cited all sources from which I obtained data, ideas, or words that are copied directly or paraphrased in the document. Sources are properly credited according to accepted standards for professional publications. I also certify that this paper was prepared by me for this purpose.

Student's Signature: _____Corland G. Keating_____