Analyzing Information Security Model for Small-Medium Sized Businesses

Full papers

Yazan Alshboul
Dakota State University
yaalshboul@pluto.dsu.edu

Kevin Streff
Dakota State University
Kevin.streef@dsu.edu

Abstract

As large organizations invest heavily in security frameworks, cyber criminals and malicious insiders are turning their attention to smaller businesses to steal or damage sensitive information. Unlike large enterprises, small businesses often pay little attention to hackers, cyber criminals, and malicious insiders. Furthermore, small-medium sized organizations are challenged to implement proper information security strategies due to insufficient resources. Very few methods and publications focus on information security for small and medium sized organizations.

This paper reviews the National Institute of Standards and technology (NIST) framework for security in small and medium-sized businesses. After discussing several concerns with NIST's approach, our proposed methodology is introduced and examined to provide an information security framework suited for small and medium sized businesses.

Keywords

Security frameworks, NIST, risk assessment, cyber security, security model in small and medium sized organization.

Introduction

Small and medium sized organizations are those organizations that employ between 1 and 500 employees (NISTIR 7621 2009). In the fact, small and medium sized enterprises constitute more than 95 percent of all businesses in the United States as well as produce around 50 percent of the United States' income (NISTIR 7621 2009). Therefore, it is important to increase the awareness of information security responsibilities of small and medium sized organizations to protect valuable system and information resources for the nation.

With the global proliferation of computerized information systems, small and medium sized organizations akin to large organizations use information systems to automate their tasks and distribute their products and services. This movement toward the interconnected information world highlights the importance of conducting information security research and implementing security strategies to keep these organizations safe from cyber attacks.

It is crucial for small and medium sized organizations to protect their customers' sensitive data like healthcare information, credit card information and personal information. Furthermore, a company needs to protect its intellectual property, marketing data and its valuable information like strategic plans, financial information, and marketing reports to maintain its reputation and to remain competitive.

Large organizations have matured their investment in information protection resources including technology, people, processes, and budgets to improve the security of its valuable and sensitive information. On the other hand, small and medium sized organizations do not have such equivalent resources to build a solid information security framework. Therefore, hackers and cyber criminals have recently focused their attacks on small and medium businesses after they find that large organizations are difficult targets to attack and have well secured infrastructure (Beachboard et al. 2008). Furthermore,

lacking security policies and procedures make small and medium sized businesses susceptible to attacks by insiders who have direct access to the information systems of the organization (Beachboard et al. 2008).

Small and medium sized organizations find it difficult and costly to implement one of the existing information security frameworks like NIST 800-53, ISO/IEC 27001, OCTAVE, or ITIL due to lack of resources and the size of these frameworks. While these standards are marketed for all sized organizations, the reality is that these frameworks are simply too large and complex for small organizations to understand and operationalize. In this regards, the Information Technology Laboratory of the National Institute of Standards and Technology (NISTIR 7621 2009) provides a security fundamentals framework developed exclusively for small businesses and therefore takes into consideration the unique needs of this audience. For example, the cybersecurity framework necessary for Walmart would be significantly different than a four-person law firm on main street Iowa. NISTIR 7621 documents security practices all small businesses should adopt to provide basic security for information and information systems.

In this paper, we discuss and analyze the NISTIR 7621 framework and propose a new methodology to be used by small and medium sized enterprises using the NIST special publications SP 800-39 for risk management and SP800- 53 for risk assessment (NIST SP 800-30 2012; NIST SP 800-39 2011). This paper is organized as follows; the third section discusses related work, Section 4 outlines NIST's fundamental actions and recommendations, Section 5 addresses the shortcomings of the NIST 7621 model, while Section 6 discusses our proposed methodology of information security for small and medium sized enterprises. Finally, we conclude our work.

Related Work

In the 21st century, most organizations are using information technology to automate tasks, provide services to customers, and store sensitive customer and company data. Therefore, organizations must be prepared to prevent and mitigate any threat to steal non-public information (McCumber 2005). The dissemination of information technology in most of the sectors generates new threats against information assets and information technology. These threats may cause damage and destruction for the organizations. In order to protect organizations from these threats, governments highlight the importance of managing the security threats and the necessity of regulating information security within the organizational level (Sloms and Solms 2008). In this context, the United States' government realizes the necessity for regulating the using of information technology, and issued Presidential Decision Directive 63 to protect the critical digital infrastructures in the United States (Clinton 1998). Furthermore, the White House considers cyberspace security as a priority that should be governed (Fischer et al. 2013; NIST 2014; Obama 2013; The Whitehouse 2009) through the establishment on information security programs in organizations.

As the foundation for an information security program, many information security frameworks are available for organizations to use. These frameworks support risk management processes, risk assessment processes, auditing, and implementing risk-based security controls. One of these frameworks is the NIST framework which is initiated by the National Institute of Standards and Technology (NIST SP 800-53 rev4 2013). NIST is an organization concerned with many aspects related to security and quality of life in terms of the Federal Information Security Management Act (FISMA) (public law 107-347 2007). The NIST framework provides a set of information security controls in the context of the risk management process to specify the security requirements of the organizational, functional, and information system level. According to the risk assessment, the security controls are selected and tailored to the organizational security needs. According to Cumber (McCumber 2005), a key element of the information security process is to establish a risk assessment process. A risk assessment process aims to identify and analyze information risks in order to prevent or mitigate them. A risk assessment process also includes identifying the information assets and analyzing threats that may act on the vulnerabilities of the organization through estimating the probability of threat occurrences and the impacts of reasonably foreseeable threats. While the NIST 800-53 document is thorough, it is deemed overwhelming for most small organizations and finds its primary audience being U.S. government agencies.

Another information security framework available was developed by the International Standards Organization (ISO) (ISO/IEC 27001 2005). ISO/IEC 27001 provides guidelines for the best practices to initiate, implement, and improve information security management systems. There are four phases of the ISO/IEC 27001 standards namely plan, do, check, and act (PDCA). ISO 27001 is typically used in Fortune 5000 organizations.

Furthermore, the Office of Government Commerce of the United Kingdom issued Information Technology Infrastructure Library (ITIL) (OGC service strategy 2011) as a standards checklists for integrating IT services with the organization's strategy. ITIL depends upon the ISO/IEC 2000 which include the IT international service management standards. The ITIL framework can be used as a foundation for an organization's security program, but like the ISO standard is typically used in large, corporate environments.

Others have studied the issue of information security frameworks in small and medium sized enterprises. Gupta and Hammond conducted a study about information technology and information security issues in small firms in both manufacturing and services (Gupta and Hammond 2005). They refer that there is limited research in the area of information security issues in small businesses. In their research, Gupta and Hammond mailed a questionnaire to 1000 small businesses owners. They found that small business owners do not use a standard framework and make up their own information defense strategy (Gupta and Hammond 2005). Beachboard et al. proposed an open development information security strategy to conduct risk analysis for small and medium sized enterprises (Beachboard et al. 2008). Their proposed methodology included four security initiatives namely:

- Develop a multi-level IA risk analysis methodology and decision heuristics.
- Develop decision heuristics for quantification of organizational costs.
- Develop and maintain knowledge base of probability estimates associated with threat classes.
- Develop automated tools instantiating the analysis methodology, heuristics, and knowledgebase.

Streff and Podhardshky developed a risk management framework for small and medium-sized business which is in use in banks today, but it does not prescribe specific security controls for small businesses to deploy (Lovaas and Streff 2009; Podhardsky et al. 2011; Streff et al. 2009). It also automates many of the decisions small enterprises need to make but lacks a repeatable process. Moyo, Abdullah, and Nienaber studied the information security within South African secondary schools (Moyo et al. 2013) and found that secondary schools use computerized information systems that include sensitive data about educators, learners, creditors and financial records which must be protected and that school management must become more aware of information security issues in their computerized information systems. They used and customized the OCTAVE risk management methodology to conduct security risk management in two selected schools in South Africa. OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) is a suite of tools, techniques, and methods for risk-based information security strategic assessment and planning (OCTAVE 2003). This approach is considered a comprehensive approach but it is too time consuming and difficult for small businesses to use.

Hillston proposed four information security tips to minimize the risks of data breaches in small businesses (Hillston 2013). Gene Marks discussed how to protect a business using frameworks against a data breaches (Marks 2013) by providing seven ways to protect any small business against data breaches. In a similar context, David Mielach argues several issues concerning small businesses and data breaches (Mielach 2012). Hillston, Marks and Mielach's work contributes but lacks a repeatable process to bake security into the culture of an organization.

In summary, while many tips, best practices, and frameworks exist, nothing in the marketplace merges together a prescriptive list of controls with a repeatable process to bake security into a company through a repeatable mechanism. Further, many of the aforementioned are simply too large for small enterprises to adopt. This paper outlines the first framework that leverages prescriptive controls in a repeatable process that is right for the small or medium-sized organization.

Prescriptive Control Model: NIST's Fundamentals of Information Security for Small Businesses

Organizations can either come up with their own list of security controls to implement via a risk assessment process or be prescribed which security controls they need to implement. For example, the banking sector must complete a risk assessment and determine which security controls they want to implement. This also holds true for most industries including oil & gas, food, and healthcare. Conversely, the government agencies are prescribed which security controls to implement based on the risk rating of the system. This "prescriptive control" approach provides more consistency in control selection and is also valuable when security experts are not on staff to make risk-based control decisions. Since small businesses typically lack security experts, the prescriptive approach seems appropriate for this subset of institutions.

Recognizing that the prescriptive approach may be helpful to small business, the Information Technology Laboratory of the National Institute of Standards and Technology (NIST) issued a prescriptive-based information security guide specifically for small businesses: NIST Interagency Report (NISTIR) 7621, Small Business Information Security: The Fundamentals. The report authored by Richard Kissel, NISTIR 7621 presents three major areas that small businesses should address: essential information security practices, highly recommended practices, and other planning considerations. Traditional risk assessment involves the business identifying security threats, calculating probabilities and impacts, to determine necessary controls to mitigate risk to an acceptable level. The NISTIR 7621 standard assumes that small business lack the requisite resources to complete this function, so instead prescribes specific actions all small business should take (Essential Practices) and further lists ten additional actions small businesses should consider (Highly Recommended Practices). NISTIR 7621 prescribes ten absolutely necessary security controls to secure information in small businesses. The premise for the NISTIR 7621 standard is to itemize for small businesses the specific security controls they should implement as most small business lack the skill to discern whether they should first implement a firewall or improve personnel screening methods. Table 1 outlines the 10 Essential Practices.

Antivirus
Internet Security
Firewall
Patching
Backups
Physical Security
Wireless Security
Employee Awareness
Individual User Accounts
Limiting Access

Table 1: NIST 7621 Essential Practices.

The Essential Practices include: Protect information/systems/networks from damage by viruses, spyware, and other malicious code, Provide security for your Internet connection, Install and activate software firewalls on all your business systems, Patch your operating systems and applications, Make backup copies of important business data/information, Control physical access to your computers and network components, Secure your wireless access point and networks, Train your employees in basic security principles, Require individual user accounts for each employee on business computers and for business

applications, Limit employee access to data and information, and limit authority to install software. These are the first ten actions a small business should invest in to secure their business.

The Highly Recommended Practices augment the Essential Practices list for a business that desire to go beyond basic security to further fortify their network and organization. The highly recommended practices include: Security concerns about email attachments and emails that requesting sensitive information, Security concerns about web links in emails, instant messages, social media, or other means, security concerns about popup windows and other hacker tricks, Doing online business or banking more securely, recommended personnel practices in hiring employees, issues in downloading software from the internet, security considerations for web surfing, how to get help with information security when you need it, how to dispose of old computers and media, and how to protect against social engineering. These security controls should only be implemented after all Essential Practices are put in place. See Table 2 for a list of highly recommended practices.

Email Security
Web Security
Pop-up Windows
Online Business
Hiring Practices
Downloading Software
Web Surfing
Getting Help
Equipment and Media Disposal
Social Engineering

Table 2: NIST 7621 Highly Recommended Practices.

NISTIR 7621 Shortcomings

NISTIR 7621 provides the basic security controls that can be implemented by small business management (NISTIR 7621 2009). However, most of the NISTIR 7621 focuses on the technical security issues for small enterprises like installing firewalls, patching operating systems, antivirus, and backing up business data. While the standard does a nice job prescribing these essential security controls, we see that it is as important (or likely even more important) for small business management to better understand information security of their businesses from a security management perspective rather than from technical perspective where they can find technical security procedures from many resources. The thought here is that for small business owners to really embrace and invest in security controls, they need to set the tone at the top (FFIEC 2014) through establishing a repeatable process. For example, an Acceptable Use Policy which outlines management's direction regarding acceptable use of technology at the business is an important security step which is not detailed in NISTIR 7621 but likely should be so that management is working together to outline acceptable practices.

Just as large businesses, many small businesses look to contract with many technology vendors; therefore third party risk management is an important component of any information security framework. Most small businesses don't create their own hardware or develop their own software. In their report for small business information security, NIST does not focus on how to manage third party risk management. This issue has proven large for many industries, including banking and healthcare (Bulletins 2013; Hinkley et al. 2014). Furthermore, NIST does not refer to the importance to document a security strategy for small

businesses. In the following section, we suggest an information security architecture for small businesses in terms of (NIST SP 800-30 2012; NIST SP 800-39 2011) and in terms of NIST's fundamentals.

A New Information Security Model for Small Business Organizations

The two issues described in the previous section are addressed by creating a new information security model for small business organizations that levarages the prescriptive control work of NISTIR7621 and several of the other security standards which purport a repeatable security process. The proposed methodology consists of the four phases from the ISO 27001 framework and the prescriptive controls documented in NISTIR 7621. More explicitely, the four phases of Plan, Do, Check, and Act (PDCA) are integrated with the NISTIR 7621 10 absolutely necessary and 10 highlighy recommended controls to build a comprehensive framework for small and medium-sized businesses. Figure 1 presents the four phases of the proposed security model for small-medium busineses.

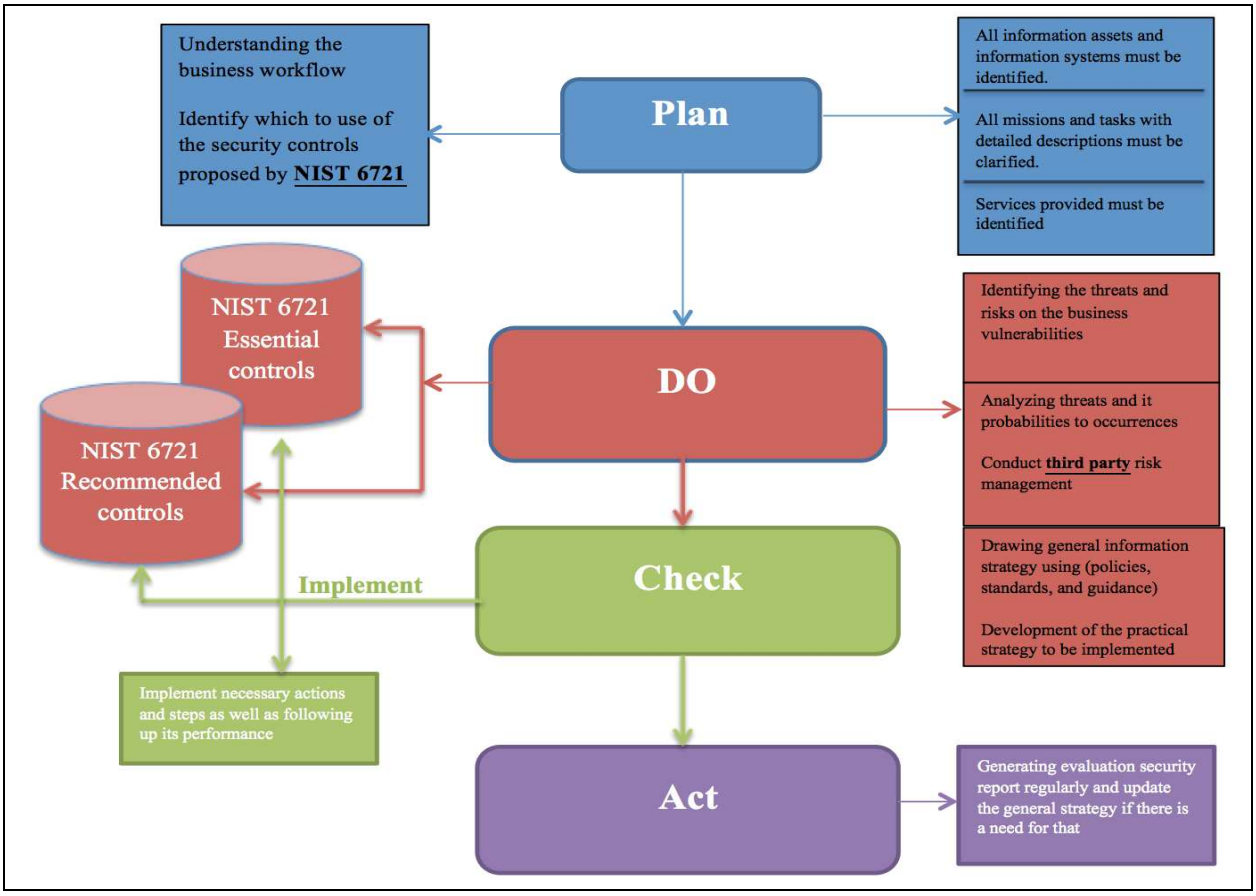

Figure 1: Security Model for Small-Medium Businesses.

Phase 1: Plan

Business owners must devise a security policy that outlines the importance of information protection and the steps they will follow to secure their informiaton and systems. The ISO 27001 framework addresses Asset Management as one of the security domains and we have included this concept into our small business information security framework. In the plan phase, small business owners should identify information assets and information systems that are used to accomplish the business missions. Furthermore, small business owners must specify the tasks assigned to each employee to determine what the information that the employee need to access in order to accomplish the assigned task. This phase is

not described well in NIST's fundemental report for small businesses. We believe that this phase is important to establish any information security framework.

Phase 2: Do

In Phase 2, business owners determine whether they are going to implement only the essential controls identified in Table 1 or also the highly recommended practices outlined in Table 2. While all businesses must implement the controls outlined in Table 1, some businesses may feel this is insufficient and want to do more. Table 2 outlines further control options. The "Do" phase also deals with the vendor management program as most small businesses rely heavily on vendors for hardware, software, support, hosting, etc. In fact, small business management has to identify the vendors who store, process, or transmit non-public information. Third party management did not mentioned in NIST 6721 report. In this phase, business owners have to draw the general information strategy to be implemented in the business security strategy.

Phase 3: Check

After identifying information assets, understanding security controls, and enumerating technology vendors, Phase 3 includes small businesses implementing the controls identified in Phase 2. Owners and managers must see evidence that these controls were implemented, which is why this phase is called "check". For example, they may review the Acceptable Use Policy, look for evidence that a firewall was installed, or request a review of the contract for that important vendor. Furthermore, small businesses may implement the necessary actions and steps as mentioned in the previous two phases (Plan and Do phases).

Phase 4: Act

In this phase, security strategy components that mentioned above are implemented in a form of a well-designed documentation in details. Furthermore, the absolutely necessary actions mentioned in NIST's report might be implemented in the implementation phase. This phase should include a report that consists all the vulnerabilities and how to protect it against any possible attack. Regarding security awareness, this phase should consists of training programs and training schedules to improve employee' awareness of information security. Also in this phase, small business owners have to review the information security framework on a periodic basis to ensure that the control framework is keeping pace with the threat landscape. This is one of the real deficiencies in using the NISTIR 7621 framework by itself is that management may implement the 10 absolutely necessary controls, but if the threat landscape changes and they don't stay on top of it then their business is put at risk. Further, NISTIR 7621 is a living document; meaning, NIST is on version 2 of the standard. If the organization does not have a process to continually review, then they may not implement the newest version of the standard in their organization leaving their information and systems vulnerable.

Conclusion and Future Work

This paper concluded that which many information security frameworks are available, all frameworks have fatal flaws that leave a small business unable to fully implement, leaving the organization open for attacks. This paper put forward a new framework that addressed the fatal flaws of existing frameworks and described this framework for many small businesses to use. We recommended a melding together of the prescriptive approach and the phased approach, and specifically recommended using the PDCA phased approach with the NISTIR 7621 prescriptive approach.

As for future work, we are testing our proposed framework at small and medium sized organizations through implementing our security framework in a bid to analyze the effects and the usability of the framework within small and medium sized organizations. Furthermore, we will conduct an empirical study of the proposed framework in order to evaluate, enhance, and improve it is applicability for the target audience and measure the improvements over existing approaches.

REFERENCES

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

Bulletins. 2013. "Third-Party Relationships:," *Office of the Comptroller of the Currency: US department of the Treasury* (available at http://www.occ.gov/news-issuances/bulletins/2013/bulletin-2013-29.html).

Clinton, B. 1998. "Presidential decision directive 63," *The Whitehouse , Washington, DC* (63) (available at http://www.dtic.mil/dtic/tr/fulltext/u2/855356.pdf).

FFIEC. 2014. "FFIEC cybersecurity assessment general observation," *Federal Financial Institutions Examination Counsil* (available at http://www.ffiec.gov/press/PDF/FFIEC_Cybersecurity_Assessment_Observations.pdf).

Fischer, E. a., Liu, E. C., Rollins, J. W., and Theohary, C. a. 2013. "The 2013 Cybersecurity Executive Order: Overview and Considerations for Congress," *Congressional Research Service*, pp. 1–22 (available at http://www.fas.org/sgp/crs/misc/R42984.pdf).

Gupta, A., and Hammond, R. 2005. "Information systems security issues and decisions for small businesses: An empirical examination," *Information Management & Computer Security* (13:4), pp. 297–310 (doi: 10.1108/09685220510614425).

Hillston, G. 2013. "4 Information Security Tips Every Small Business Owner Should Know," *Tweek your Biz* (available at http://tweakyourbiz.com/technology/2013/09/10/4-information-security-tips-every-small-business-owner-should-know/).

Hinkley, G. A., Briskin, C., and Bloom, C. 2014. "Omnibus Final Rule Issued on HIPAA / HITECH Act : Significant Changes for," *Pillsbury Winthrop Shaw Pittman LLP* (available at http://www.pillsburylaw.com/siteFiles/Publications/AlertFebruary2013HealthCareFinalRuleIssuedonHIPAA_HITECHACT_SignificantChangesforBusinessAssociates.pdf).

ISO/IEC 27001. 2005. "Information technology – Security techniques – Information security management systems – Requirements," *International Organization for Standardization*.

Lovaas, P., and Streff, K. 2009. "A Comprehensive Information Technology Risk Assessment Audit Framework for Small- and Medium-Sized Financial Institutions," in *Proceeding of the Fourth Midwest United States Association for Information Systems Conference*, Honolulu, HI.

Marks, G. 2013. "7 Ways To Protect Yourself Against A Data Breach," *Forbes* (available at http://www.forbes.com/sites/quickerbettertech/2013/12/31/7-ways-to-protect-yourself-against-a-data-breach/).

McCumber, J. 2005. *Assessing and managing security risk in IT systems* (2nd editio.), Auerbach Publications, ISBN 0849322324.

Mielach, D. 2012. "What Small Businesses Need to Know About Data Breaches," *Fox Business-small business center* (available at http://smallbusiness.foxbusiness.com/technology-web/2012/09/04/what-small-businesses-need-to-know-about-data-breaches/).

Moyo, M., Abdullah, H., and Nienaber, R. C. 2013. "Information security risk management in small-scale organisations: A case study of secondary schools computerised information systems," *IEEE*, Ieee, pp. 1–6 (doi: 10.1109/ISSA.2013.6641062).

NIST. 2014. "Framework for Improving Critical Infrastructure Cybersecurity," *National Institute of S*, pp. 1–41 (available at papers2://publication/uuid/DD40979D-D391-4678-9601-F14CF1CB8BF5).

NIST SP 800-30. 2012. "Guide for conducting risk assessments," *National Institute of Standards and Technology, NIST*.

NIST SP 800-39. 2011. "Managing information security risk," *National Institute of Standards and Technology, NIST*.

NIST SP 800-53 rev4. 2013. "Security and privacy controls for federal information systems and organizations SP 800-53 rev 4," *National Institute of Standards and Technology, NIST*.

NISTIR 7621. 2009. "Small business information security : The fundamentals," *National Institute of Standards and Technology, NIST*.

Obama, B. 2013. "Executive Order -- Improving Critical Infrastructure Cybersecurity," *The whitehouse, President Barak Obama* (available at http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity).

OCTAVE. 2003. "Introduction to the OCTAVE Approach," *Carnegie Mellon Software Engineering Institute* (August) (available at http://www.itgovernanceusa.com/files/Octave.pdf).

OGC service strategy. 2011. "ITIL version 3: Service strategy," *Office of Government Commerce*.

Podhardsky, A., Streff, K., Pauli, J., and Engebretson, P. 2011. "A Restructured Information Technology Risk Assessment Model for Small and Medium-Sized Financial Institutions," in *Hawaii International Conference on Business (HICB 2011)*, Honolulu, Hawaii, USA.

public low 107-347. 2007. "Information security," *Federal Information Security Management Act of 2002* (48:sec 301), pp. 48–63.

Sloms, S. H. Von, and Solms, R. 2008. *Information security governance* (1st ed.), Springer.

Streff, K., Lovaas, P., and Podhardsky, A. 2009. "A Progressive Information Security Program Model for Small and Medium-Size Financial Institutions," in *Hawaii International Conference on Business*, Honolulu, Hawaii.

The Whitehouse. 2009. "Cyber space oolicy review: assuring a trusted and resilient information and communications infrastructure," *The Cyber Security Social Contract: Policy Recommendations for the Obama Administration with Congress* (available at http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf).