European Journal of Business and Management
ISSN 2222-1905 (Paper) ISSN 2222-2839 (Online)
Vol.12, No.18, 2020

An Integrated Framework for Managing Information Technology Security Uncertainty

Weian Wang[1*] Li Luo[2]
1.Department of Computer and Information Science, Hartwick College, 1 Hartwick Drive, Oneonta 13820, USA
2.Department of Business Administration and Accounting, Hartwick College, 1 Hartwick Drive, Oneonta 13820, USA
* E-mail of the corresponding author: wangw@hartwick.edu

Abstract
Information security to date has been driven a lot of attention in business world. The cyber security standards play significant and crucial role in promoting feasible approaches to organizations while making comprehensive strategical planning. This paper aims at providing a systematic overview of information technology (IT) security management in organizations. Conducted a structured literature from academic database and industry whitepapers, we review a number of the critical issues and challenges facing the industry today and in the future. In line with the fundamental elements of information security, we propose an integrated framework to understand the current situation of IT security management. In particular, we focus on several critical fundamental functions of IT security management: Security and Risk Management, Security Operations, and Security Assessments and Testing. Then, we use the proposed framework as a lens to discuss and solve the security issues in bring your own device (BYOD) in organizations.
Keywords: IT security, IT security framework, bring your own device
DOI: 10.7176/EJBM/12-18-01
Publication date: June 30th 2020

1. Introduction

The rapid development in information technology (IT), the accessibility it offers, and ease of use have contributed to an increasing tendency for organizations to invest in developing information systems (Jones et al., 2005). IT has changed the way organizations run businesses in the 21st century (Sidelinger et al., 2008). Since the internet has been widely implemented into modern business processes, organizations are more susceptible to potential attacks on their information systems (Bojanc and Jerman-Blazic, 2008; Silva et al., 2014). These attacks may lead to security failures that cause huge losses (e.g., market failure) for companies (Chen et al., 2011). IT security continues to be a priority and a critical challenge for organizations (Luftman et al., 2016). As a result, more and more business enterprises develop and implement different risk management governance mechanism, while managing corporate information security such as intelligence-based information security framework (Webb, 2015), fuzzy-based information security framework (Silva et al., 2014), and risk-based information security framework (Bojanc and Jerman-Blazic, 2008). Therefore, IT security has become an essential part of strategic proportions for an organization. For example, many organizations applied the Failure Mode and Effects Analysis (FMEA) in identifying flaws of key processes in the operation level since it offers a set of measures and comparison, as well as provides an effective way to build business process knowledge (Silva et al.,2014).

The purpose of this paper is to provide a systematic overview of information technology security management in organizations. We review some of the critical issues and challenges facing the industry today and in the future, as well as three of the fundamental functions of information security. In doing so, we utilize the three principles of information security: confidentiality, integrity, and availability (Khansa and Zobel, 2014). To identify critical challenges, we concentrated on the three primary functions of security management: Security and Risk Management, Security Operations, and Security Assessments and Testing. We chose to define these functions because they provide the necessary security services expected from a business management point of view. Additionally, if appropriately executed, these security functions have a high return on investment for businesses. Therefore, we develop an integrated framework for the management of IT security through incorporating industry-leading security framework.

The organization of this paper is as follows. In section 2, we discussed the methodology for the study. In section 3, a literature review of information security is discussed, and a holistic view is developed based on risk management perspective. Next, in section 4, we proposed an integrated framework for information security management. In the next section, we discuss and analyze BYOD security concerns based on our proposed framework in section 4. Finally, the paper is concluded.

2. Methodology

We used a structured literature review as a methodology to analyze to understand the nature of security management. Specifically, we paid particular attention to search industry best practices, peer reviewed research,

recent media articles, and personal experiences to provide a summarizing look at the security environment and how it supports the overall business organization. We further analyze our research to posit on the problems and challenges that three of the top security issues (i.e., Security and Risk Management, Security Operations, and Security Assessments and Testing) will pose on Information Systems Management and business as a whole. Our research identified some of the most significant trends affecting the security industry are also some of its biggest challenges.

Since we selected to review the literature, we conducted a comprehensive search. As proposed by Webster and Watson (2002), this research is not limited to a specific journal and tries to cover all relevant literature. This research is focused on the published papers in peer-reviewed journals that are developed frameworks, as proposed theories for information security. This goal is pursued in two steps. In the first step, a number of keywords were identified to start the search with them. The search process started within important electronic databases, including Science Direct, Web of Science, Academic Search Premier, and white papers available in the leading practice websites (e.g. onlinetech.com). We started our search by trying "IT security" and "Framework". Using different keyword combinations of these groups, several seminal papers were found. Then we found new papers based on the seminal papers that we referenced to. In the second step, the citations in each collected paper were reviewed to identify other potential related papers.

3. Information Security from a Risk Management Perspective

The phrase "information security" in the business context is a broad term and has been expressed into different aspects such as technology (Li and Guo, 2007), people (Dhillon and Backhouse, 2001), and protection process (Bishop, 2003). As such, a business organization to manage information security is the process of managing IT-based risk. Given the pervasiveness of IT into every aspect of business process in the organization, IT risk has become more important in corporate risk management (Hunter and Westerman, 2007). IT risk may "damage corporate reputations and expose weaknesses in companies' management teams. Most importantly, IT risk dampens an organization's ability to compete" (Hunter and Westerman, 2007).

3.1 Principles of Information Security

Information security is required through a set of processes that contain policies, standards, mechanisms, governance, and practices. All of these controls aim to achieve three core goals of information security: Confidentiality, Integrity, and Availability. The three principles together are also called the CIA triad, which is a model for making information security policies within an organization (Khansa and Zobel, 2014). Business organizations in many industries use the CIA triad as guidelines for their analysis, evaluation, planning, and implementation of their corporate information security (Lopez and Oliveira, 2014).

Confidentiality refers to the company protecting their information assets by restricted authorized entities (Keung, 2014; Lopez and Oliveira, 2014). The company is required to ensure the authority for different groups of users (Lopez and Oliveira, 2014). For example, executives are authorized to access all corporate information, while employees are only authorized to access information associated with their jobs. Integrity refers to the company protecting its information assets from unapproved modification (Keung, 2014; Lopez and Oliveira, 2014). The company should ensure integrity that corporate information (e.g., data) cannot be edited without any authorized permit (Khansa and Zobel, 2014). For example, if integrity can be violated easily, employees are able to change their salary in the corporate accounting systems. Availability refers to the company protecting its corporate information asset from unapproved interruption (Keung, 2014; Lopez and Oliveira, 2014). The company should ensure the availability of information systems to meet their needs in a timely manner (Keung, 2014). Also, the system should be reliable for access and usage (Khansa and Zobel, 2014).

3.2 Security Operations and Investigation

The objective of security operations is threefold. First, it provides a process that allows an organization to manage its overall security operations. As part of this process, organizations are able to develop mechanisms that allow security staff to investigate and decide on policies and methods used on the security operations, based on the analysis of the potential benefits and level of risks (Helen Morris, 2012) Second, it allows the organization to understand and evaluate how the security operations provided enable it to achieve desired outcomes. It will also establish a mechanism for tracking how security operations can respond to risks in an organizational environment (Helen Morris, 2012). Finally, it provides control over which services are offered with what level of security and under what conditions (Helen Morris, 2012). In order to develop a comprehensive security operation overview, we consider an investigation, incident management, and disaster recovery in this section.

It is often the case that security operations initiatives are unsuccessful when corporations ignore the processes and attempt to fix the problem right after it occurs. Security operations must include the standards and policies, which may require adaptation of best-practice methods for the individual circumstance. It is vital to have a consistent approach for people at all levels of the organization. The organization must begin with setting a clear

strategy and defining the policies that drive the way it will be achieved. With those policies in place, organizations will be able to control the way they carry out their security operations (Morris, 2012).

Effective investigations will help to reduce guesswork by revealing associations hidden in the data. Those associations are useful for security operations. The security team will respond appropriately to mitigate or eliminate threats and uncover meaningful patterns. For security investigation, the processes can be summarized as data collection, monitoring and analysis, and solutions. Corporations use different methods and tools to make the business safer. Monitoring, data intake, and initial response are the essential responsibilities of enterprise security operations. Data gathering would be the first step in the investigation. Security management relies on a data-driven decision. During this stage, corporations will gather and extract information from the vast amount of available data. The security team will ensure that they will collect incident data consistently and accurately. Then they will analyze these data to derive useful information about security issues and educate upper management about the variety and intensity of threats to the corporations. Organizations can take advantage of data to produce usable insights to guide their decisions. These insights will be used to support activities across the entire organization (McIlravey, 2015).

3.3 Incident management and disaster recovery

Effective incident management will improve availability, ensuring that users will get back to work quickly following a security problem. An incident management approach would have helped to resolve the issue in a shorter amount of time. Project teams with a good understanding of policies and procedures help provide a realistic assessment of business impact. (Helen Morris, 2012). The effect of this incident is to delay the project and dissatisfy the internal customers. The project leader decides to address the issue to the stakeholders and documents it as lessons learned. Due to the impact of this case, incident management is visible to the business and demonstrates its value. The company defines its incident management process to control better vendors to increase service availability by reducing service downtime.

A disaster is defined as a severe disruption of the functioning of a company. Nature disaster is deemed as a common disaster, which includes floods, hurricanes, earthquakes, and volcano eruptions that have immediate impacts on human health and enterprise operations (Wcpt.com, 2014). Organizations must recover operations should any type of disaster occur. A detailed disaster recovery plan should be reviewed on a quarterly basis. Consider this scenario, you are a service manager in charge of operations for a larger manufacturer. In the early morning of a business day, you receive a phone call from an engineer, saying there was an earthquake in his region, several systems were impacted. He is waiting for your instructions and guidance. In this case, you need to follow the disaster recovery plan to assess and remedy this situation.

3.4 Security assessment and testing

An analysis of Security Management is not complete without an understanding of a robust Security Assessment and Testing program. Security and risk management enables a business to meet regulatory issues and provides a minimum standard of compliance. Asset Security directly hardens the end devices that are most susceptible to a loss of Confidentiality, Integrity, or Availability. However, Asset Security does not necessarily focus on the businesses' most critical assets or key infrastructure. Security Operations assist in rectifying any incidents that occur on a network quickly and efficiently. This leaves Security Assessment and Testing as the sole program to identify problems and make security improvements to the information systems in a way that prioritizes key infrastructure and critical assets that have been identified by the Security and Risk Management program of an organization.

For a security assessment and testing program to be successful, the test must include a gamut of automated scans, tool-assisted tests, and manual efforts to challenge the security, as hackers will have equal access to all of these capabilities. Additionally, tests must occur regularly but not set schedules, thus ensuring specific information systems are not neglected, and tests do not occur on easily predicted days every month or quarter. However, the frequency and depth of the test should correspond to the business value of the system to the organization. For example, if BYOD is one of the organization's critical resources for performing essential functions of business, then the security team should prioritize test to focus on these devices. Many other factors should be considered when scheduling testing. There are only so many security testing resources available. Thus, it might behoove management to conduct limited automated scans on less valuable assets and full scans with manual oversight on increasingly critical applications. Almost counterintuitively, certain intense scans have the potential to cause harm to an information system due to stress or technical failure, causing loss of availability, and should be carefully selected when applied to critical systems and only conducted during authorized periods of service interruption, previously agreed upon with business management. (Stewart et al., 2015)

An administrator cannot only conduct an automated scan of a critical system and conclude a test. A thorough review of the test must be performed, and the results logged and analyzed for potential vulnerabilities. Once the review has been completed, an assessment report is created that details the success or failure of the test, the findings,

and the recommended corrective actions. Additionally, the report also presents the threat environment to that specific system and the current and future risks (Stewart et al., 2015). Finally, the security assessment report must include perspective into the company's security posture weighted against technology-specific standards. Yet, it must also be presented in a way that management can plainly understand the risks and proper recommendations (Krause and Tipton, 2006).

3.4.1 Security Assessment

There are two main types of vulnerability scans; network vulnerability and web vulnerability. Some tools can do both types of scans. Nmap is one of the most popular open-source tools for conducting basic network scanning. Nmap has the ability to scan a subnet and identify the current state of ports on a network. Additionally, utilizing the OS detection setting, Nmap can determine essential characteristics of what operating systems are running on a network. (Shaw, 2015) While Nmap does not provide all of the use cases for a network assessment, it is undoubtedly a good start. Nessus, on the other hand, incorporates Nmap into its network vulnerability assessment and goes several steps farther. Once the network has been enumerated with Nmap scans, Nessus can conduct any number of tests on the web. In simple terms, it does this by probing open ports for known vulnerabilities in its database.

When the probe results in success, Nessus provides a report to the administrator. Similar to network vulnerability scanning, Nessus also provides web vulnerability scanning. The main difference between the two is that the web vulnerability scanner is generally able to probe deeper into the configuration of the webserver as compared to the network assessment probe of individual hosts. (Stewart, J. M., Chapple, M., & Gibson, 2015). These tests can support patch management and can determine if there are any systems on the network out of compliance with the latest updates. Also, Nessus supports scheduled test that can be run regularly without the need for manual intervention (Kumar, 2014).

While the information security manager is not going to be the individual configuring NMAP and Nessus scans, it is crucial to understand the necessary capabilities and limitations of the most common industry-accepted tools. Like vulnerability assessments, penetration tests also have their own unique set of industry-accepted tools. A penetration test is a legal and authorized attempt to exploit vulnerabilities on an information system or network. (Engebretson, 2011) Generally, a penetration test targets a specific system or systems and utilizes a gamut of tools and tactics to gain access and demonstrate a flaw. Like vulnerability assessments, the end game is to provide a detailed report of all the flaws identified during the test and provide recommendations for hardening.

3.4.2 Security Testing

There are three different types of penetration tests. White box testing is conducted within the organization. In this test, the security professionals conducting the test are completely familiar with the network. Black box testing is the opposite and represents a test in which the attackers have no information about the network prior to conducting the penetration test. Gray box testing is some combination of the two (Muniz, Lakhani 2013). An excellent example of this is the Department of Defense's new "Hack the Pentagon" bug bounty program. This gray box test, in which the organization provides details of the authorized target network and implements rules and regulations to vetted hackers, represents a new trend in cybersecurity. Through the use of crowdsourcing, organizations pay white hat hackers to test their system in a way that creates a more secure network. (U.S. Department of Defense) These tests provide cash payouts in the thousands of dollars to participants who are able to find vulnerabilities on an organization's network. In many cases, these have a direct business advantage, saving potentially millions of dollars spent on cleaning up a compromise or paying for credit monitoring services for customers after a data breach.

As with vulnerability scanning, an information security manager needs to understand what tools are available and the different phases of the test. Many penetration testing tools are open source and can potentially save businesses thousands of dollars compared to comparable proprietary software. One such example is the penetration tool kit known as Kali Linux. Kali is a Linux distribution designed to provide tools for each level of a penetration test. It would be an exhausting exercise to detail all of the tools available at each level, so we will merely provide the different phases of a penetration test. The first phase is surveillance, in which the penetration tester develops an understanding of the target network with various scanning tools. The second step is the target evaluation. The penetration tester may utilize the same tools available in a vulnerability scan, such as Nessus, to evaluate a target for weakness. In the third phase, the attacker attempts to obtain a foothold using exploitation tools such as Metasploit. In the fourth phase, the goal is to escalate privileges and potentially gain root level or administrative level privileges to a system. The final step is to maintain a foothold establishing multiple access methods and removing evidence of access (Muniz, Lakhani 2013). As with vulnerability scanning, a penetration test is not complete without a full report of access gained and recommended mitigating actions. Both types of test assist an information security manager in maintaining a high level of confidentiality, integrity, and availability, thus increasing overall business performance.

4. Developing an Integrated Information Security Framework

In order to achieve the three core objectives of information security, a number of information security risk management frameworks are presented in this section. We develop an integrated security framework (Table 1) based on the NIST Cybersecurity Framework, and the IBM information security capability reference model are presented in this section. The NIST framework focuses on the principles of Identify, Protect, Detect, Respond and Recover. In contrast, the IBM framework stresses the principles of People and Identity, Data and Information, Application and Process, Network Server and Endpoint, and Physical infrastructure. We choose these two frameworks because they are industry best practices applied across different industries. On the other hand, these two actionable frameworks provide metrics that allow us to understand security management from a holistic overview. Table 1 presents a combined framework based on two security frameworks.

Table 1. Integrated Framework of Information Security Management

NITS Cybersecurity Framework		IBM Security Framework: Security Governance, Risk Management and Compliance				
		People and Identity	Data and Information	Application and Process	Network, Server and Endpoint	Physical Infrastructure
Identity	Asset Management					
	Business Environment	Supports globalization of operations				
	Governance		Provides a cost-effective way to meet legal discovery, hold and retention requirements		Readily show status against major regulations	
	Risk assessment			Automated testing and governance throughout the development lifecycle, reducing long-term security cost		
	Risk Management					
Protect	Access Control		Assures data is available to the right people, at the right time	Ability to integrate business critical application	Increases productivity by decreasing risk of virus, worm and malcode infestation	
	Awareness and Training					
	Data Security	Decreases risk of internal fraud, data leak, or operational outage				
	Information Protection Process and Procedures	Reduces the cost, increasing efficiency and enables auditability of managing flow of users entering, using and leaving the organization	Reduces the costs, increases ability to meet audit and compliance mandates Decreases number and complexity of controls integrated within the enterprise			Integrated physical security surveillance strategy allows extracting intelligent data from multiple sources, respond to threats sooner than manually monitored environments, and reduce cost and risk of loss
	Protective Technology			Reduce risk of outage, defacement or data theft associate with web applications		Reduce risk of outage or data theft associated with failure or loss of critical physical assets

NITS Cybersecurity Framework		IBM Security Framework: Security Governance, Risk Management and Compliance				
		People and Identity	Data and Information	Application and Process	Network, Server and Endpoint	Physical Infrastructure
Detect	Anomalies and Events		Assures data is not deliberately or inadvertently taken, leaked, or damaged			
	Security Continuous Monitoring			Assess and monitor enterprise-wide security policy compliance	Reduces cost of ongoing management of security operations	
	Detection Process	Enables shift from traditional brick & motor sales to delivery of on-line services to customers and partners across the globe				
Respond	Communication					
	Analysis				Decreases volume of incoming spam	
	Mitigation					
	Improvement	Improves end-user experience with Web-based business applications by enabling such activities such as single sign-up		Improve compliance with industry standards and regulatory requirements (for example, PCI, GLBA, HIPAA, FISMA, and so on)	Improves operational availability and assures performance against SLA, backed by industry's only guaranteed SLA for managed protection services	
Recover	Recover Planning		Decreases number and complexity of controls integrated within the enterprise			
	Improvements				Drill down on specific violations to quickly address resolution	
	Communications					

5. Scenario Case Study: Bring Your Own Device

Bring Your Own Device (BYOD) is one of the primary digital transformation for business due to its simplicity and inexpensive costs (Wang and Nemati, 2016). The BYOD strategy allows employees, business partners, and others to personally select which devices they would like to use to effectively maximize their needs for the company and needs for themselves (Wang and Nemati, 2016). Due to the increase of supply of these services, higher demand for security is needed, and the future trends of BYOD equate to higher standards of education and training. Currently, IT leaders have been using the BYOD adoption, and most IT leaders have a positive view upon BYOD, and they see it as inevitable (Yabubu, 2013). It is known that BYOD improves employee satisfaction, and that result is a pleasant experience for CIOs and their organization (Yabubu, 2012). However, some of the most significant challenges facing security are ironically also some of its greatest assets.

5.1 BYOD Security Challenges

End to end encryption, BYOD policies are some of the hottest topics in IT security today. Risk management, well-managed security operations, and regular security assessments can help to alleviate these challenges. More importantly, BYOD is a way to access information that isn't owned and managed by the IT department (Yakubu, 2013). BYOD can be a problem due to the control and security of corporate data being in the hands of employees and the possibility of sensitive data being exposed (Yakubu, 2013). On the other hand, BYOD can increase work

efficiency and flexibility by allowing employees to work from anywhere (Yakubu, 2013). Challenges for the future of BYOD are the security risk due to the possibility of sensitive data getting into the wrong hands.

In addition, BYOD policies are a particularly unique challenge for security (Wang and Nemati, 2016). Until recently, giving employees the choice of bringing their own devices to use in the workplace would have been such a security concern it would have been unimaginable. However, as corporations increase their use of mobile devices, the need to have this choice is becoming increasingly demanded and required. With the increasing demand for access to an organization's data using personal devices that are not managed by an IT department, multiple types of threats that can prove detrimental to an organization have ascended.

Initially, IT staff attempted to defend these mobile devices using the same type of software they used for computer terminals. The problem with this approach was that there are too many different types of mobile operating systems to make this practical. To mitigate this developing security risk, companies have begun incorporating mobile device management (MDM) software. MDM software is software that is installed on employee's devices to prevent the installation of malicious apps. It also provides encryption of sensitive data and attempts to segment the personal data on the device from the business data. However, installing software onto employee's own devices may introduce grave privacy concerns regarding the separation of corporate and personal data. Consider when an individual leaves the organization. How do we know they are not going to take corporate secrets with them on their way out? On the other hand, the privilege to use their own device to access sensitive corporate data means that they will have to give up certain aspects of privacy for secure access (Stewart et al., 2015).

5.2 Possible Solutions Via Framework

According to the framework, organization need to implement encryption mechanisms in accordance with their business process. Encryption provides confidentiality and integrity. While you might be thinking to yourself, "how can encryption present a challenge for security professionals?" you must consider the fact that encryption reduces the visibility of traffic on the network. Sensors that used to produce alerts for malicious web traffic are much more restricted. Security administrators that we're able to implement data loss prevention software to detect insider threats or corporate espionage have a much more difficult time with the amplified use of end to end encryption. Utilizing qualitative risk frameworks and quantitative measurements, security management must decide how to mitigate this risk. One of the options is to implement an expensive host-based security system that can see through end to end encryption and identify threats at the endpoints. Additionally, security teams should conduct regular security assessments in which penetration testers attempt to exfiltrate encrypted information bypassing standard network sniffing tools. While these options are supportive, encryption will continue to evolve and security administrators must learn to adapt.

In addition, organizations can also use framework to lookup relevant software for securing their devices. Like all critical IT infrastructure and key resources, but especially newly incorporated software, businesses should implement a rigorous security assessment and testing strategy for BYOD. Finally, the company must ensure they are prepared to conduct security operations on the given devices if necessary. Specifically, this means developing standard operating procedures for conducting investigations on an individual's personal device. Not only do we have to consider the confidentiality and integrity of the data on the device but also the availability to the user. With that said, BYOD may actually improve security operations as it could provide an alternate means for the business to function during disaster operations.

6. Conclusion

Security is an ever-evolving challenge for management (Luftman et al., 2016). As such, information systems professionals should be broadly familiar with the many management and planning issues that involve the security domain (McKeen and Smith, 2012). So this study attempts to provide a comprehensive understanding of IT security management for business organizations. Combined two market leading security frameworks (i.e. NIST and IBM), we use this integrated framework as a lens to understand current situation of IT security management. In particular, we focus on a number of critical fundamental functions of IT security management: Security and Risk Management, Security Operations, and Security Assessments and Testing. We believe that these functions provide the fundamental security services expected from a business management perspective. If these security functions are executed appropriately, an organization would have a high return on investment for businesses. We suggest that future work could be focused on strengthening the framework into an individual organization, contributing more insights regarding information security management for specific purpose.

References

Alissa Torres (2015), Building a world-class security operations center: A roadmap, https://www.sans.org/reading-room/whitepapers/analyst/building-world-class-security-operations-center-roadmap-35907

Bojanc, R., & Jerman-Blažič, B. (2013). A quantitative model for information-security risk management.

Engineering Management Journal, 25(2), 25-37.
Brian McIlravey (2015), Streamlining Operations and Investigations with Incident Management Tools, http://www.securitymagazine.com/articles/86047-streamlining-operations-and-investigations-with-incident-management-tools
Charlotte Brooks, Matthew Bedernjak (2002), Disaster Recovery Strategies with Tivoli Storage Management, http://www.redbooks.ibm.com/redbooks/pdfs/sg246844.pdf
Chen, P. Y., Kataria, G., & Krishnan, R. (2011). Correlated failures, diversification, and information security risk management. Mis Quarterly, 35(2), 397-422.
Choo, Kkr. "Cloud Computing: Challenges and Future Directions." Trends and Issues in Crime and Criminal Justice 400 (2010): 1–6. Web.
Dhillon, G., & Backhouse, J. (2001). Current directions in IS security research: towards socio-organizational perspectives. Information Systems Journal, 11(2), 127-153.
Engebretson, Patrick. Basics of Hacking and Penetration Testing. Syngress, 2011. 10 April 2016 http://www.myilibrary.com?ID=316445
Eric Cole (2015), Why security operations centers are the key to the future, http://searchsecurity.techtarget.com/tip/Why-security-operations-centers-are-the-key-to-the-future
Helen Morris, Liz Gallacher (2012), ITIL Foundation Study Guide, John Wiley & Sons, Ltd.
Hunter, R., and G. Westerman. (2007). IT risk: turning business threats into competitive advantage. Boston: Harvard Business School Press.
Jones, A., & Ashenden, D. (2005). Risk management for computer security: Protecting your network & information assets. Butterworth-Heinemann.
Keung, Y. H. (2014). Basic Principle of Information Security. Advances in Robotics & Automation, 2014.
Khansa, L., & Zobel, C. W. (2014). Assessing innovations in cloud security. Journal of Computer Information Systems, 54(3), 45-56.
Krause, Micki, and Harold F. Tipton. Information Security Management Handbook. [London]: CRC Press, 2006. eBook Collection (EBSCOhost). Web. 9 Apr. 2016.
Kumar, Himanshu. Learning Nessus for Penetration Testing. Birmingham, GBR: Packt Publishing Ltd, 2014. ProQuest ebrary. Web. 10 April 2016.
Lebin Cheng, Ravi Ithal, Krishna Narayanaswamy, and Steve Malmskog. "Cloud Security for Dummies." (2015): John Wiley & Sons, Inc.
Li, Y., & Guo, L. (2007). An active learning based TCM-KNN algorithm for supervised network intrusion detection. Computers & security, 26(7), 459-467.
Lopes, I., & Oliveira, P. (2014). Understanding information security culture: a survey in small and medium sized enterprises. In New Perspectives in Information Systems and Technologies, Volume 1 (pp. 277-286). Springer International Publishing.
Luftman, J., & Ben-Zvi, T. (2011). Key issues for IT executives 2011: cautious optimism in uncertain economic times. MIS Quarterly Executive, 10(4), 203-212.
Mandal, S., & Maiti, J. (2014). Risk analysis using FMEA: Fuzzy similarity value and possibility theory based approach. Expert Systems with Applications, 41(7), 3527-3537.
MobileIron. MobileIron Product Packaging. N.p.: MobileIron, n.d. Web. <https://www.mobileiron.com/sites/default/files/datasheets/files/MobileIron%202014%20Bundle%20Datasheet_V2-0_EN.pdf>.
Muniz, Joseph, and Lakhani, Aamir. Web Penetration Testing with Kali Linux. Birmingham, GBR: Packt Publishing Ltd, 2013. ProQuest ebrary. Web. 15 April 2016.
Onlinetech.com (2016), benefits of disaster recovery in cloud computing, http://www.onlinetech.com/resources/references/benefits-of-disaster-recovery-in-cloud-computing
Ozkan, S., & Karabacak, B. (2010). Collaborative risk method for information securitymanagement practices: A case context within Turkey. International Journal ofInformation Management, 30, 567–572.
Puhakainen, P., & Siponen, M. (2010). Improving employees' compliance through information systems security training: an action research study. Mis Quarterly, 757-778.
Shaw, David. Nmap Essentials. N.p.: Packt., n.d. ProQuest. Web. 10 Apr. 2016.
Silva, M. M., de Gusmão, A. P. H., Poleto, T., e Silva, L. C., & Costa, A. P. C. S. (2014). A multidimensional approach to information security risk management using FMEA and fuzzy theory. International Journal of Information Management, 34(6), 733-740.
Stewart, J. M., Chapple, M., & Gibson, D. (2015). CISSP: Certified information systems security professional study guide. Indianapolis, IN: Sybex, a Wiley brand.
Tim Mather, Subra Kumaraswamy, and Shahed Latif. 2009. Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance. O'Reilly Media, Inc..
U.S. Department of Defense. Statement by Pentagon Press Secretary Peter Cook on DoD's "Hack the Pentagon"

Cybersecurity Initiative. Defense.gov. N.p., 02 Mar. 2016. Web. 15 Mar. 2016.
Vladimirov, Andrew, Gavrilenko, Konstantin, and Michajlowski, Andriej. Assessing Information Security. Cambs, GB: IT Governance Publishing, 2010. ProQuest ebrary. Web. 9 April 2016.
Wang, W., & Nemati, H. (2016). Understanding Usage of Bring Your Own Device (BYOD): A Complex Adaptive Systems Perspective.
Wcpt.com (2014), what is disaster management, http://www.wcpt.org/disaster-management/what-is-disaster-management
Webster, J., & Watson, R. T. (2002). Analyzing the past to prepare for the future: Writing a. MIS quarterly, 26(2), 13-23.
What We Do: Simplify Enterprise Mobility. N.p.: AirWatch, n.d. Web. <http://www.air-watch.com/downloads/brochures/airwatch-solutions-overview.pdf>.
William Long (2013), BYOD: data protection and information security issues, http://www.computerweekly.com/opinion/BYOD-data-protection-and-information-security-issues
Yakubu. "Cloud Computing and BYOD : Benefits and Challenges in Modern Healthcare." November 2013 (2016): 24. Print.
Zafar, H., & Clark, J. G. (2009). Current state of information security research in IS. Communications of the Association for Information Systems,24(1), 34.