Information Security Management – Current Threats, Challenges, & Mitigations

Mark E. Turner

East Carolina University

Abstract

Security threats continue to present challenges to both private and public sectors. Evidence of this problem is provided in daily news reports of data breaches involving private citizens data. Information security Management (ISM) has become the largest growing field within Information Technology (IT) as a result. With funding being increased for the sole purpose of addressing these threats and the challenges associated with mitigating them, it is important to maintain an up to date and relevant understanding of current trends within this field.

This paper will provide an overview of established information security management principles. These concepts will then be reviewed to form a baseline knowledge of understanding and create a literature review. Potential threats were reviewed for relevance and were identified as either external or internal. Challenges were attributed to either Recruitment, Organizational, or Infrastructure issues. The authors goal is to provide an overview of current threats and challenges to help new and current IS professionals to better understand the subject and provide solutions where relevant.

Keywords: Information, Security, Management

Information Security Management - Current Threats, Challenges, and Mitigations

Security breaches in major companies and institutions continue to be a hot topic in the news, as well as with both government and corporate leadership. Continual attacks against these organizations generate fear and panic in both internal and external stakeholders. Roberts (2018) explains that the average cost of a data breach in 2018 is $3.3m dollars. This size of a loss forces down the valuation of a company or ends political careers for government leaders. General citizens begin to dread the steady drip of negative news associated with these breaches and lose faith. Therefore, many different methods have been deployed to protect and promote security with a focus on managing these potential challenges. The most significant of these is the management and security of information.

Information security management also known as InfoSec has become the fastest growing field within Information Technology. Significant funding has been raised in the private sector to promote this growing field. It was reported recently by TechCrunch (2019) that in 2018, Information security startups accounted for over $5 Billion worth of investment startups to address this need. With cyberterrorism rates rising, ISM has become a constant focus of governments. This has led to the redirection of government funding from traditional military spending to cyberwarfare investments. is field is tasked with the goal of promoting security for resources and protecting information about customers and members.

McCandless (2016) tells us that over $6.6 Billion was invested in IT education spending in 2016 in the U.S. alone.. Educational degrees have been designed to promote knowledge of ISM, and to train the next generation of professionals. The toolsets and methods taught within these institutions has evolved from threats that have arisen over the last two decades. While, many of these threats are still valid, some no longer pose an immediate threat. Yet the

mitigations used to address these older threats still make up a main component of formal training. New threats continue to arise in this field regularly and it is important to be informed and current. These new threats pose challenges to daily operations, as well as deploying necessary countermeasures to mitigate them. But, how can we create mitigations to address these new challenges and threats if we don't effectively understand how they are tied together? The author will provide an understanding of these current threats and the challenges associated with mitigating them within the scope of ISM.

This paper will provide an overview of established information security management principles. A brief overview of these concepts will then be reviewed to form a baseline knowledge of understanding and create a literature review. An explanation of ISM principles will be directed towards specific standards and challenges mandates by current regulatory bodies. All sources will be reviewed with the intent of using only internationally recognized journals and organizations such as those released by the Institute of Electrical and Electronics Engineers (IEEE). To prevent the use of stagnant facts, only sources that have been released in the last three years will be used to provide an up to date and relevant review of the current literature.

Potential threats were reviewed for relevance and were identified as either external or internal. Challenges were attributed to either Recruitment, Organizational, or Infrastructure issues. Potential frameworks or standards will be acknowledged but not covered in depth to maintain the scope of the report. This paper is written for an audience of Information Security professionals with a foundation of basic security and technology knowledge. Conceptual illustrative figure and relevant data will be provided to assist the reader when possible. The author will provide questions for future research and expansion of the subject. The authors goal

is to provide an overview of current threats and challenges to help new and current IS professionals to better understand the subject and provide solutions where relevant.

Literature Review

Information security management has come to be considered a unique and specific field for over 15 years. During this time technology has grown and the concept has evolved. ISM is primarily used to ensure the CIA (Confidentiality, Integrity, Availability) triad of security for assets are maintained. Collard, Disson, Ducroquet, & Talens (2017) states values of assets are important when referencing the CIA and when this is successful assets are protected. Whether this is from vulnerabilities that can be acted upon by a threat agent or unknown threats. To protect all assets a risk management system must be enacted to provide an assessment of asset risk.

Assets are identified and their valuation to the company assessed. The amount of risk associated with each asset is directly tied to how vulnerable they are to an attack or potential vulnerability. Almutairi & Riddle (2017) explain that risk assessment is only as strong as the threat assessment process. They go on to explain that threats should directly form the risk assessment process. a threat as A plan is then drawn up by the management team in order to determine what countermeasures or mitigation are available. Associated costs of the mitigation are weighed against the risk of the attack to determine risk matrix.

While risk management is a significant component of information security management, likelihood of a threat occurring is weighed against the impact of the losses from the occurrence. From this result a measurement of risk is created and assigned to each of the individual assets. Anttila & Jussila (2017) explain that risk controls must be aligned with business goals. An IS

manager can then prioritize which of the assets is at greatest risk and can then address it. How risk can be addressed is dependent on the mitigation cost. If a cost is too much for a specific business model then the risk is absorbed and essentially ignored. Risk can also be transferred by simply insuring against the effects, much like traditional consumer insurance. Finally, mitigation costs can be increased or decreased dependent on the type of solution being implemented. Small amounts of mitigation can provide some minimization of risk. In the end, risk can be decreased, but not removed. To completely remove all risk, the business component would need to be abandoned or worse the mitigation would be cost-prohibitive. The next step is to integrate the management of risk and assets into the organizational structure.

Information security management systems (ISMS) are a formalized method of taking specific assets and business specific processes and integrating them together. Brunner, Sillaber, & Breu (2017) directs us that this integration is systematic and is directly influenced by the needs of the business. Business needs must be preserved, or the implementation of security will simply choke out the company. Therefore, in order to address an organization needs and objectives, individual processes must be prioritized as well as assessed to determine their impact on asset security. The complexity of this can become very difficult to manage. Luckily there are available plans known as security frameworks designed to solve different problems.

Security frameworks are essentially strategies designed around a specific level of security, business need, or government mandate. Each of these frameworks involves asset and risk assessment. Followed with risk monitoring enforced by a specific plan, a manager can then determine and assign risk metrics to individual processes, assets, or business needs. These metrics are then monitored by key personnel who are assigned to report specific datapoints on a routine basis. It is important to note that according to Anttila & Jussila (2017) the effectiveness

of these metrics will only be as accurate as the personnel collecting them. The organization must require these metrics be viable and accurate.

Metrics are then collated into a viewable format and provided to key stakeholders. These stakeholders then review and determine if change or improvements will be effective to the existing metrics. Finally, results are reported to the executive management team. The executive team will then determine if updating the existing framework is needed. There are many different frameworks that have specific goal sets. Although our focus will be on the current changes planned for two of the most well-known standards. We will begin with Control Objectives for Information and Related Technologies (COBIT).

COBIT 2019

COBIT was created by the Information Systems Audit and Control Association (ISACA). This organization was concerned with the creation of a general purpose or well-rounded framework that was logical and easily implemented within an existing business structure. One of the key development points was that it should be easily accessible at all levels of the organization. Collard, et al. (2017) also informs us that operational functionality is tied to the functionality of the framework used. Components were designed to supplement IT while allowing for a business to perform normal operations freely. Because of its easily deployed tools the architecture was designed to supplement other frameworks very easily.

The first version was released in 1996 known simply as COBIT, and subsequently updated to version 5 in 2012. There have been several changes to COBIT for this version. Some of the changes are available in Figure 1 below. One of the biggest complaints about COBIT was that the development cycle was too sporadic and often lagging behind other framework models.

ISACA chose to solve with this when they released COBIT 2019 earlier this year. Improved metrics for security modeling and subsets are intended to allow for improved integration into existing frameworks and organizational structure. Interaction with other frameworks allows for a layered and multi-structured approach to security management.

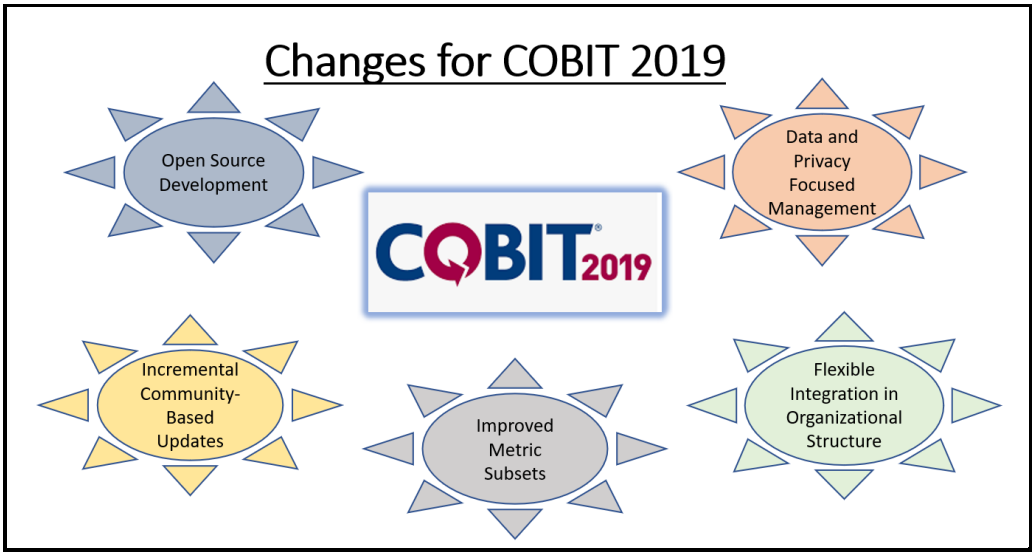

Figure 1 – Changes for COBIT 2019

Enhanced coverage of data security and privacy management tools. Because of the need for integration with existing projects and the Software Development Life Cycle (SDLC), integration with existing project management toolsets allows for better coordination. ISACA (2018) explains that because of the lack of user input from previous iterations, COBIT will now be developed towards an open source model. This will allow for constant updates and improvements to follow along with existing security management programs. From the open source model users are expected to provide regular feedback to ISACA in order to create a better product. These changes have caused many people to state that COBIT has been improved far better than many of its competitors. We will now reference the SP 800-53 framework released by NIST.

NIST SP 800-53 Revision 5

The National Institute of Standards and Technology (NIST) is a federal agency under control of the United States government. As directed by Federal law, NIST has created several publications that dictate regulation and control of data within the US government and between third parties. To cover each of these would be outside the scope of this paper, but when referencing security frameworks NIST Special Publication (SP) 800-53 dictates required security frameworks to be utilized when managing or controlling access to federal data.

The publications primary focus is on the use of a Risk Management framework with the goal of selecting and assigning risk through the use of security controls, impact analysis, and mitigation controls. There have been several revisions to this publication, but what is important to IS professionals is the fifth and latest revision of the regulations. These final revisions are being released later in the summer of 2019. Current draft revisions are being circulated so as to gather feedback consensus on the changes. Many of these changes are shown in Figure 2 below.

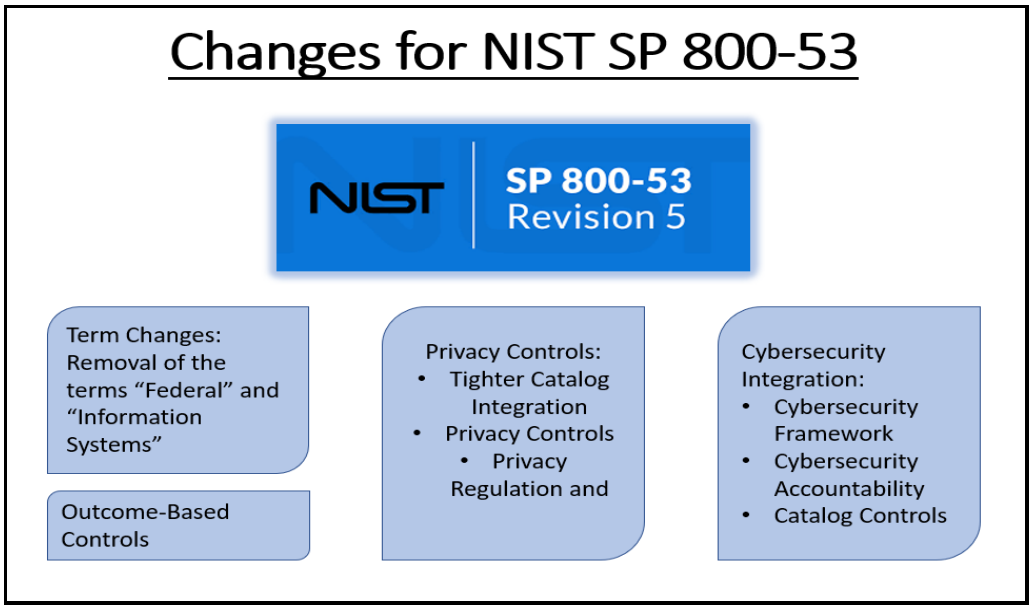

Figure 2 – Changes for NIST SP 800-53

Several changes have been implemented in order to promote adoption among international companies. Other changes include the direction of the controls being focused towards other applications other than IS. This will allow for adoption amongst more corporate companies. Integration of privacy controls by placing them into the metrics catalog will make privacy just as important as security. With more of a focus on Personally Identifiable Information (PII), this will create a baked-in approach to privacy.

Several changes have been included to update the control catalogs to provide for an enhanced delivery model. Implementing a focus of outcome-based structures within the control subsets will allow for a direct and specific outcome. Previous revisions were considered to be too vague in the delivery of control outcomes. Several of the catalog changes are directly focused on threats from cybersecurity intrusions and privacy accountability such as those found in the European Union (EU) regulations, the General Data Protection Regulation (GDPR). According to NIST (2019) the biggest changes as noticeable by the bulk of the changes is the focus on privacy and data management.

As with most changes being enacted, industry follows regulation. Much of the ongoing changes being enacted over the next few months will be focused on data, privacy, and PII. The brutal reality is that with the adoption of the GDPR, there will be significant “catch-up” by industry standards to adopt a reactive stance. This is due mainly to the legality of failing to meet the standards in place by this regulation. Standardization and even international regulatory boards such as NIST will be forced to accept and implement the necessary changes. Failure to meet this goal will force ISMS managers to either look for alternatives to deploy within their organizations. These changes are the most significant to come out of a regulatory body since the

Federal Information Security Management Act of 2002 (FISMA). After reviewing the literature, we will now turn our attention to the current threats and challenges to IS management.

Discussion

To effectively review current threats, it is necessary to categorize these threats as either internal or external threats. This is necessary due to recent breaches and the threat agents that enacted them. By categorizing them it is far simpler to review challenges associated with them. For the purposes of this paper, internal threats will include all personnel within an organization as well as third-party agents that are used to complete daily business. With this assumption, all agents of third parties are considered to have been exposed to some form of security or vetting process. All other threats will be considered external threats. We will begin with internal threats and describe current issues associated with them.

Internal Threats

More than ever before companies are looking inward for threats than outward. Whether they are examining employees, infrastructure, or software, concerns are refocused from problems arising over the last few years. Almutairi & Riddle (2017) warns us that human threats could be accidental or even unintentional. In other words, the result may not be what was originally intended, but these outcomes can be highly detrimental to a business. Most often these threats can be solved with simple processes to improve security and prevent issues. Insider-backed breaches by employee mistakes is one of the leading causes of security concerns within the Information Security space. As these topics are covered. we will focus our attention to three types of challenges and potential mitigations for solving them. These three areas are Personnel,

Organization, and Infrastructure challenges. We will take a look at Recruitment first as human threats are the biggest threats of the three.

Personnel Challenges

Human threat agents make up the largest component of internal threats, and mitigating this challenge is not easy. This is mainly due to identifying these issues is extremely difficult. Intentional threats are often linked to insider information trading, sabotage, intellectual theft, political leakers, and even whistle-blowers. Edward Snowden is one of the most famous leakers in IT. Insider Threat detection is extremely difficult and Alotibi, Clarke, Li, & Furnell (2018) explains that technology makes it easier for these threats to occur. With current Bring Your Own Device (BYOD) policies it is difficult to police these devices due to privacy issues.

It is very easy for any of these threats to smuggle out information or smuggle in a virus. The easiest methods for mitigating these threats is the use of enforced access policies for network access or to deny access to networks at all. For devices that are company issued, these devices can be seized or even frozen. Alotibi, et al. (2018) also suggests the use of advanced firewall techniques and Deep Packet Inspection (DPI) of all traffic. Finally if necessary, the use of Faraday cages in highly secure areas for personal devices is optimal as well.

Other issues stemming from personnel is the use of third-party staff that collaborate on projects and other areas. Almutairi & Riddle (2017) even suggest the use of hybrid management models including the use of remote and expanded security systems to monitor and enforce security policies on subsidiary or partner systems. While this is considered to be a potentially effective method it can be intrusive. Brodin (2017) suggests that the costs associated with the provision of mobile devices can provide access to devices that can ensure integrity of data and

processes as well as protect confidentiality. Managing employee technical mistakes is managed through the implementation of review processes and accountability verification. By creating systems that require a layered approval process to prevent mistakes or errors, this small cost will provide a return on investment (ROI) very quickly. We will not turn our attention to organization challenges.

Organization Challenges

There are two primary challenges from an internal organizational threat. The first is the threat of the sharing of Information Security data. As companies outsource particular components of their business it is imperative to enforce organizational requirements on the outside company. Wang, Herwono, Di Cerbo, Kearney, & Shackleton (2018) cautions against complete data sharing between companies. They suggest that the use of managed security services with a focus on privacy and data protections. An example of the dangers of this is the recent enforcement of the GDPR on several companies. An associated company can mishandle data on your behalf, and this could still lead to your organization being in direct violation of this regulation. Zibak & Simpson (2018) even suggest that direct observation or co-mingling of teams could be used to prevent this. The direct method is cost efficient but creates a breakpoint on a single area. Therefore, the use of third-party security management simply for the exchange of data with the third-party is recommended as a mitigation.

The second threat is the issue of financial exchanges between organizations. Every company must have some type of sales mechanism, even for the sale of service. How data nd finances are handled will be a direct issue in the next few years as new currencies such as BitCoin and cryptography transactions are more difficult to trace and reverse if necessary. Kushwaha, Bibhu, Lohani, & Singh (2016) have warned over time that digital crime from sales

or hacking have recourse within current regulatory rules. Cyber laws have not kept up with the current crop of cryptographic monetary systems. As a result, this can create a serious threat when exchanging these types of currencies between companies. Until international and domestic laws catch up to these issues, there is no mitigation and the threat can lead to highly expensive mistakes.

Infrastructure Challenges

The most significant threat in the coming years is the threat associated with wireless sensor network. Whether the sensors are being used for robotic automation or for improved access such as Internet of Things (IoT) devices, these present the most significant challenge moving into the next decade as hackers become increasingly proficient at hacking these devices. Liang, Liu, Yao, Yang, Hu, & Ling (2017) warns us that rogue nodes from unpatched and forgotten devices are definite threats. Due to the low cost associated with these devices, a deploy and forget method is often dangerous. Only when these devices are problematic do they become noticed.

An ISMS with a specific policy directed towards regular update tracking will provide an effective mitigation to these issues. While automation requires an initial capital investment, the ongoing maintenance of these devices is mandatory in order to prevent threats from becoming a reality. Brunner, Sillaber, and Breu (2017) warns that simple audit systems are not effective and that to properly integrate automation, management tools or deployment systems should be used. An example of a framework that could be used to mitigate this is the ADAMANT framework and how it is very reliable when used with IoT devices. One of the newer technologies that could be used to mitigate this challenge is the use of Software Defined Networks (SDNs). Varadharajan, Karmakar, Tupakula, & Hitchens (2019) suggest that deployment of this

architecture lends itself extremely effectively to management of diverse and large networks such as IoT devices and networks found in automation industries.

Over-reliance on existing network infrastructure that is outdated or even obsolete is dangerous as well. While it is a necessity that the power grid is consistently relying on significantly aged equipment, planned updates and even investment planning is possible through the use of an effective ISMS. Chen (2018) has explained that the use of Risk Management to mitigate threats to the Smart grid is effective and cost effective. Effective deployment of an ISMS is suggested as the most effective mitigation for this threat as well. Now that we have covered all of the Internal threats we will not turn our attention to External threats.

External Threats

As more data breaches are recorded daily, external threats are still a viable and potentially devastating threat to a company in ISM. Most often these are unknown threats and come form threat agents that are often located across international boundaries. With no international laws to prevent these attacks there is often no way to recover what was stolen. Especially when it is data not financial assets. Potential loss of sales and respect within an industry can be difficult to return from when it happens. Therefore, we will group challenges from this type of threat into two categories: Criminal, and Cyberterrorism. We will begin with Criminal challenges as this is the most prevalent of the two.

Criminal Challenges

Criminal threats are difficult because of the diversity of attacks and the players involved. The most significant of these are denial of service, financial theft attacks, and data breaches. Denial of Service (DoS) attacks have been an ongoing problem for over two decades. In the last

5 years the attacks are now delivered as a component of activism and malfeasance. Belov, Pestunov, & Pestunova (2018) explain that disruption to business processes is difficult to prevent and often difficult to recover from. Until recently many of these attacks were simply to gain attention. Attacks have been directed at companies with the intent of preventing access to service. An attack was directed at a DNS provider and an entire regions access to the internet was disrupted as a result of the attack. Moving forward these types of attacks will be directed more at infrastructure backbones of the Internet.

Financial theft attacks will never cease. There will always be threat agents with the goal of stealing funds if possible. Yoon & Kim (2017) explain that the key provider on a network is the security management server. If this device is taken down then this can create an even bigger issue for the network. Oftentimes this type of attack is coordinated with some type of DoS attack. Mitigations for this type of threat are simply to keep up to date devices and software. Additional protections can be to limit specific types of traffic to the servers and to whenever possible prevent access to key components. Criminals with the intent of theft require a defense in depth and even the use of third-party service providers such as Cloudflare. This is another example of transferring risk.

Data breaches are significant and often impossible to recover from due to the ensuing legal troubles that a company encounters when they occur. Mengke, Xiaoguang, Jianqiu, & JianJian (2016) explain that big data can provide many benefits, but the unfortunate reality is that securing data repositories is oftentimes impossible dependent on the footprint of the network and the number of locations that are involved. Mitigations for this type of attack are best left to the use of Network Intrusion Detection Systems (NIDS) and secondary security systems such as stateful firewalls. With the right update policies in place as well as updates being deployed

regularly, these types of attacks should be few and far between. While zero-day exploits are common for hardware and software vendors, the failure to patch when once is available is the biggest threat.

Cyberterrorism Challenges

Min (2018) explains that people's everyday livelihoods are tied to access to electricity. No sector has been mentioned more by all countries as being more vulnerable to either terrorist or nation-state attacks. Cyberterrorism is divided into two groups: Espionage or terrorism. When referencing espionage there is often no way to really prove the country who has hacked or damaged your country. Therefore, these threats are more dynamic and cannot be predicted. Hong, Jianwei, Zheng, Wenhui, Xi, Hongyu, & Shengsheng (2017) explain that dynamic threats are often difficult to mitigate as the threat will come from multiple attack vectors. The most effective mitigation for this is to layer in defense and to deploy real-time monitoring systems. While an ISMS will assist in deployment and management of these resources, the actual prevention is above the reach of this toolset. This brings us to the other challenge which is terrorism.

Terrorism often has no known face, no known attack, and no known goal. These factors are often determined after the fact. While this can be frightening, the truth is that these attacks are rare. Alotaibi, Furnell, & Clarke (2016) explain that organizations that have lax or minimal security are significant targets for those who are looking for an easy target. Terrorism is often attached to the goal of maximum reward for minimum work. Therefore, the deployment of an ISMS as described in other sections is the most effective mitigation to this threat. We will now turn our attention to questions for future study.

Conclusions and Future Study

Threats to an Information Security Manager are too many to number, but many of these can be mitigated when properly prepared for. We have covered many different types of threats including internal and external threats. These can be simplified to the point of "the devil you do know versus the devil you don't". Internal threats are easily visible, while external threats are tied to often faceless agents. Challenges form these two types of threats will be difficult to manage over the next few years. The two biggest challenges will be Personnel challenges and Criminal challenges. Both of these challenges have led to some of the most significant data breaches in the past two years and they will most likely dominate the news cycle moving forward.

Questions for future study could be directed to the significance of current machine learning and the use of Artificial Intelligence in meeting some of these challenges. Other threats that will continue to be a concern is that of criminal attacks backed by nation states for the purposes of espionage. This has been a significant issue in the last few years and will continue for some time.

Finally, the reality is that there are many different challenges that the Information Security Manager will have to deal with. In reality many of these threats and challenges will be ongoing and there will be no "silver bullet" that the manager can use. Defense in depth with layered and redundant systems along with new ISMS frameworks will help the Information Security Manager to be successful as long as he is vigilant.

References

*Almutairi, M., Riddle, S. (2017). Security Threat classification for outsources IT projects, *2017 11th International Conference on Research Challenges in Information Science (RCIS*). Brighton, UK. May 10, 2017. DOI:10.1109/RCIS.2017.7956579

*Alotaibi, B., Almagwashi, H. (2018). A Review of BYOD Security Challenges, Solutions and Policy Best Practices, *2018 1st International Conference on Computer Applications & Information Security (ICCAIS)*. Riyadh, Saudi Arabia, April 4, 2018. DOI:10.1109/CAIS.2018.8441967

*Alotaibi, M., Furnell, S., Clarke, N. (2016). Information security policies: A review of challenges and influencing factors, *2016 11th International Conference for Internet Technology and Secured Transactions (ICITST)*. Barcelona, Spain. 5-7 Dec. 2016. DOI:10.1109/ICITST.2016.7856729

*Alotibi, G., Clarke, N., Li, F., Furnell, S. (2018). The Current Situation of Insider Threats Detection: An Investigative Review, *2018 21st Saudi Computer Society National Computer Conference (NCC).* Riyadh, Saudi Arabia. April 25, 2018. DOI:10.1109/NCG.2018.8592986

*Anttila, J., Jussila, K. (2017). Challenges for the Comprehensive and Integrated Information Security Management, *2017 13th International Conference on Computational Intelligence and Security (CIS).* Hong Kong, 2017, pp: 586-589. doi: 10.1109/CIS.2017.00136

*Belov, V., Pestunov, A., Pestunova, T. (2018). On the issue of Information Security Risks Assessment of Business Processes, *2018 XIV International Scientific-Technical Conference on Actual Problems of Electronics Instrument Engineering (APEIE).* Novosibirsk, Russia. Oct 2, 2018. DOI:10.1109/APEIE.2018.8545573

*Brodin, M. (2017). Security strategies for managing mobile devices in SMEs – A theoretical evaluation, *2017 8th International Conference on Information, Intelligence, Systems & Applications (IISA)*. Larnaca, Cyprus. Aug 27, 2017. DOI:10.1109/IISA.2017.8316387

*Brunner, M., Silaber, C., Breu, R. (2017). Towards Automation in Information Security Management Systems, *2017 IEEE International Conference on Software Quality, Reliability, and Security (QRS)*. Prague, Czech Republic. July 25, 2019. DOI:10.1109/QRS.2017.26

*Chen, Y. (2018). Modeling Information Security Threats for Smart Grid Applications by Using Software Engineering and Risk Management, *2018 IEEE International Conference on Smart Energy Grid Engineering (SEGE).* Oshawa, ON, Canada. Aug 12, 2018. DOI:10.1109/SEGE.2018.8499431

*Collard, G., Ducroquet, S., Disson, E., Talens, G. (2017). A definition of Information Security Classification in cybersecurity context, *2017 11the International Conference on Research Challenges in Information Science (RCIS)*. Brighton, UK. 10-12 May 2017. DOI:10.1109/RCIS.2017.7956520

*Hong, Q., Jianwei, T., Zheng, T., Wenhui, Q., Xi, L., Hongyu, Z., Shengsheng, C. (2017). An information security risk assessment method based on conduct effect and dynamic threat, *2017 8th IEEE International Conference on Software Engineering and Server Science (ICSESS)*. Beijing, China. Nov 24, 2017. DOI:10.1109/ICSESS.2017.8343029

ISACA, (2018). COBIT 2019 Framework: Governance and Management Objectives. Retrieved from http://www.isaca.org/COBIT/Pages/COBIT-2019-Framework-Governance-and-Management-Objectives.aspx

*Kushwaha, P., Bibhu, V., Lohani, B., Singh, D. (2016). Review on information security, laws and ethical issues with online financial system, *2016 International Conference on Innovation and Challenges in Cyber Security (ICICCS-INBUSH.* Noida, India. Feb 3, 2016. DOI:10.1109/ICICCS.2016.7542350

*Liang, L., Liu, Y., Yao, Y., Yang, T., Hu, Y., Ling, C. (2017). Security challenges and risk evaluation framework for industrial wireless sensor network, *2017 4th International Conference on Control, Decision, and Information Technologies (CoDIT)*. Barcelona, Spain, April 5, 2017. DOI:10.1109/CoDIT.2017.8102711

McCandless, J. (2016). U.S. Education Institutions Spend $6.6 Billion on IT in 2016, Center for Digital Education. May 22, 2016. Retrieved from https://www.govtech.com/education/higher-ed/us-education-institutions-spend-66-billion-on-it-in-2015.html

*Mengke, Y., Xiaoguang, Z., Jianqu, Z., Jianjian, X. (2016). Challenges and solutions of information security issues in the age of big data, *China Communications*. 13/3, March 2016, pp: 193-202. DOI: 10.1109/CC.2016.7445514

*Min, W. (2018). Application of Network and Information Security Risk Monitoring and Early Warning Platform in Electric Power Enterprises, *2018 China International Conference on Electricity Distribution (CICED).* Tianjin, China, 17-19 Sept. 2018. DOI:10.1109/CICED.2018.8592580

NIST (2019). Special Publication 800-53 Revision 5 Public Draft, NIST. Retrieved from https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&ved=2ahUKEwja3fDCzL3jAhXWGs0KHdF9BFoQFjABegQIABAC&url=https%3A%2F%2Fcsrc.nist.gov%2Fcsrc

%2Fmedia%2Fpublications%2Fsp%2F800-53%2Frev-5%2Fdraft%2Fdocuments%2Fsp800-53r5-draft.pdf&usg=AOvVaw1s7cGPdz1kf30mFjoIMZRi

Roberts, S. (2018). Learning lessons from data breaches, Network Security. 18(11), November 2018, pp: 8-11. doi:10.1016/S1353-4858(18)30111-9

*Varadarajan, V., Karmakar, K., Tupakula, U., Hitchens, M. (2019). A Policy-Based Security Architecture for Software-Defined Networks, *IEEE Transactions on Information Forensics and Security (TIFS)*, 14(4), April 2019, pp: 897-912. DOI:10.1109/TIFS.2018.2868220

*Wang, X., Herwono, I., Di Cerbo, F., Kearney, P., Shackleton, M. (2018). Enabling Cyber Security Data Sharing for Large-scale Enterprises Using Managed Security Services, 2018 IEEE Conference on Communications and Network Security (CNS). Beijing, China. May 30, 2018. DOI:10.1109/CNS.2018.8433212

*Yoon, S., Kim, J. (2017). Remote Security management server for IoT devices, *2017 International Conference on Information and Communication Technology Convergence (ICTC)*. Jeju, South Korea. Oct 18, 2017. DOI:10.1109/ICTC.2017.8190885

*Zibak, A., Simpson, A. (2018). Can we evaluate the Impact of Cyber Security Information Sharing?, *2018 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (Cyber SA).* Glasgow, UK. June 11, 2018. DOI:10.1109/CyberSA.2018.8551462

TechCrunch (2019). The infosec reckoning has arrived, *TechCrunch,* New York: AOL Inc. Feb 13, 2019. Retrieved from https://techcrunch.com/2019/02/13/the-infosec-reckoning-has-arrived/?ncid=txtlnkusaolp00000616