HOLISTICA Vol 11, Issue 2, 2020, pp. 1-16 DOI: DOI: 10.2478/hjbpa-2020-0015

INFORMATION SECURITY MANAGEMENT

Sri Harsha SOMEPALLI[1]*
Sai Kishore Reddy TANGELLA[2]
Santosh YALAMANCHILI[3]

Received: February 2019 | Accepted: July 2019 | Published: August 2020
Please cite this paper as: Somepalli, S. H. et. al. (2020). Information Security Management, *Holistica Journal of Business and Public Administration*, vol. 11, iss. 2, pp. 1-16

Abstract

Information security management is a very important issue for anyone working in the field of technology, or for anyone at risk of security breach, who understands the implications of these vulnerabilities. Many organizations are always on the constant threat of a security breach. It is easy for an organization to experience a data breach that can seriously compromise their data. With the evolving threats of data security, organizations are always working to ensure that their data is protected. Frameworks associated with information security can be pivotal to an organization. Frameworks employed in organizations helps to protect the employee and user information which is essential as it puts employees and clients at ease that their information is secure. Identifying the ideal frameworks for an organization is important. However, this process can be a bit tricky as a lot has to be considered to identify the best framework for the organization.

Keywords: Information Security; Security breach; Frameworks

1. Introduction

Cyber threats have been an ongoing vice in the modern world. Due to the improvements in technology, information security threats continue to increase on a larger scale and are advancing at a faster rate than what the current frameworks can accommodate. Currently, there are millions of cybercrime cases. This is due to the conductive environment to which hackers can exploit and access restricted information. The constant threat has been fuelled by the complexities in data which the current security measures fall under in terms of protecting the data.

[1] University of Cumberlands, USA, Ssomepalli8605@ucumberlands.edu
[2] University of Cumberlands, USA, Stangella8850@ucumberlands.edu
[3] University of Cumberlands, USA, Syalamanchili9054@ucumberlands.edu
*Corresponding author

Many companies have taken the initiative to protect their data using information security practices and employing staff like Chief Information Security Officer (CISO). But the question remains; are these measures adequate with the evolving threat on information security? Do companies have strategies to ensure that their data is protected? Are there adequate Information Security frameworks to ensure that threats are tackled strategically and that organizational data is secure? The following study analyses all these parameters to determine the viability of the Information security frameworks and draw experience from companies that have experienced data breaches.

The purpose of this paper is to explain information security management is, what it has to do with information security management structures. What are the information security management structures? What are the possible advantages and disadvantages of a set of information structures Security Management? Main perspectives to be taken into account in information security management and in the choice of framework, as well as the organizational factors to be taken into account when choosing the framework.

This paper main focus is on these research questions:

- What is the role of information security management?
- What are the measures of information security management?
- Are there significant and recent information security breaches?

2. Literature review

An information Security breach occurs periodically. In 2014, major companies such as Neiman Marcus, Sally Beauty Supply, Michael, PF Chang, and UPS were victims of the information breach. Because of this security violation, accountants receive personal customer information, including address, social security number, credit card numbers, accommodation information and more. Millions of people are affected by this violation. This violation has led companies to seek more information security information more securely.

Information security management was once considered as a technical problem which the IT department had to deal with. Of all these safety defects that they produce, they all worked in the business problem. The organizational leaders should ensure that everyone now knows security management information and can receive daily and related activities within the organization that affects information security.

To help IT managers and IT staff have a safe system for managing information security, they should first understand what information management information is about. Therefore, they should understand the benefits of the information security system and business benefits. There is a need to understand the advantages and disadvantages of the information security system which should be regarded as important expectations when

choosing a system of information security management and organizational matters to consider. In the context of the election. Once this is determined, the IT team and the IT department may accurately submit the security information management system chosen by an employee.

2.1. Security information management

To fully understand the Security information management rule, you must first see where it comes from. ISO, the International Implementation Organization, describes the Security information management system as the basis for "technical information management data management". It includes people, systems and IT systems in implementing the risk management process. "The systematic approach helps protect the organization against new threats, since there are many types of internal and external violations, and different strategies and information strategies are planned.

2.2. Setting up an information security system

In each organization, the Information Security Director (RSSI) is responsible for providing data identification services and data management provided by the data processing program. In the modern world, data is not stored in paper file systems, but also on PCs, network servers and other mobile devices, such as USB devices. Also, information is also transmitted through the internet, e-mail and cloud computers. So, it does not pay for a huge amount of power because it is a way to store data and information. There are three basic reasons for establishing a network of information security for this purpose. The first reason is that the law confirms the data protection law. Second, ensure the safety and processing of the company's data, and summarize, minimizing the risk and possible use of data fraud (Solms, 1998).

2.3. Basic information security (CIA triad)

Triad CIA is a very useful example of information security, namely Confidentiality, Integrity, and Availability, which is one of the largest basics of Sonia and in general, a variety of information sharing information. According to Chaeikar et al. (2012), Privacy is the ability to hide or protect information from unauthorized persons. The best practices to ensure privacy include encryption and encryption, especially when the data is transferred from one computer to another. Privacy is not limited to digital data, but also published in source format. As a result, organizations should identify potential threats, including piracy, non-incompetence, inadequate access to control and unauthorized labor activity (Métivier, 2017).

Threats are problematic for data transmission, intrusion, and anti-transmitting data during transmission. Guarantee of securities includes access control through data signals, process control through code tests, monitoring controls through record analysis and attraction controls. Separation of work and training of end users. At present, the availability of this brand per month is statistically fixed in all cases this month. The main

threats to access data disasters, bugs, web outages, the loss of time or permanence of personal opposition and humanitarian crimes (Chaeikar et al., 2012).

3. Information security frameworks

The purpose of the information and warranty secrets is that the controls are sufficient for the administration of privacy information in the municipality. Support the secrecy of information systems integrated with fat, one of the means of preparation, responsibility, governance, and control of divine humanity. The creation of the doxepin system will contribute to the establishment of a systematic system of the relativistic information society. In the United States, there is no solid structure for private organizations.

Other organizations use design technology when it comes to information security systems. Security of values implies that the introduction of various types of products for land use is caused by the necessary precautions taken by various types of devices. The security of the user at different levels is a concept that differs in the description of the data. There are several levels of encryption that provide employees with different levels of privacy. This type of framework is an institution and a guarantee of verification.

Companies can choose from multiple frameworks, but most organizations follow the GAISP, ISO, and FIPS guidelines. The Information Security Association (ISSA), a group of ten members, has developed the General Information Security Standards (PAGISP). GaisP Moren proposes to provide a complete collaboration guide between the solution and the secure access system. Another data collection system for the creation of the International Classification Agency. The ISO17799 standard can be described as "the right model for ISM vehicles and ISM troubleshooting".

One of the private privacy agencies in which an information management system can be designated, which must meet federal security standards. The public administration "Federation Protection", published as ALS FIPS publication, was created by the National Laboratory to make these procedures available to all government agencies. Everyone dies the rules and FIPS follows the staff or state 1 payment program, also must follow the FIPS guidelines.

3.1.ISO 27002

Compliance with ISO 27002 was established in 2005 by the International Organization for Standardization (ISO). In 2013, the executive received an update. ISO defined the general principle, implementation, maintenance and administration defined in one of the information security organizations (Information Shield, 2018). ISO 27002 provides a general guide to commonly accepted information security management goals. The most practical standard of ISO 27002 is a guide to the development and organizational security stations, effective security management, and building trust in business continuity across organizations. According to PECB (2018), ISO 27002 is also intended to improve the implementation of control instruments and the sale to the State of the company.

ISO 27002: 2013 has 14 main sections (PECB, 2018). These policies are:

- Section 5: Information Security Strategies: The next section describes the strategies needed to implement the information security system.
- Section 6: Information security agency: complies with the definition and function of the tasks and processes of the process and information security activities.
- Part 7: Human resource safety: ensure that employees know their roles and responsibilities in the information area.
- Section 8: Property Management: The identity of the property owner wants to be responsible for property security, property security including classification management, enrollment, and information.
- Article 9: Access control: control of access to information and information about damage, loss and other threats otherwise.
- Article 10: Translating: Use of cryptographic control to ensure confidentiality, reliability, and validity of information.
- Article 11: Physical and environmental protection: protects information protection against unauthorized access, damage, interference, loss, and damage.
- Article 12: Security: The ability of the company to provide fraud and risk reporting information accurately, accurately and securely as well as providing support, monitoring, and control of the operating system.
- Article 13: Communication Security: Protect information about networks and maintain adequate information security with external media.
- Section 14: Access, development, and maintenance systems involve collecting information systems and designing them with implementation in the development of information systems.
- Article 15: Relationship with suppliers: All property assets and access to foreign exporters must be maintained.
- Article 16: Management of information security events: effective and related strategies for dealing with information security events.
- Section 17: Business Promotion Information Business Information: Information security co-operation in business development systems.
- Article 18: Information security systems for compliance are safe and secure.

3.2. NIST

National Institute (NIST), formerly known as the National Standards Office (NBS), is the US Department of Trade Unit. NIST was established in 1901 with a view to promoting innovation in the US and industry competition and promoting science-based measurement, standards, and technology to enhance social security. The NIST structure provides guidelines on the operation of US companies. It can evaluate and improve the ability to investigate, prevent and respond to cyber-attacks. NIST first 1.0 was launched in 2014 and is a new version with version 1.1 in 2017. NIST provided classification, strategy,

customer, staff, activity, meter, analytical and educational management and results (US Department of Commerce, 2018).

3.3. COBIT

Control Objectives for Information and Related Technologies (COBIT) is a senior level structure (ISACA) created by the IT government and the management of the Association of Information Systems Control Systems. COBIT was designed as a tool for administrators to bridge the gap between technology issues, business risks, and control requirements. IT process managers around the world are used to assess organization and risk management best practices as well as to ensure the integrity of the information system. COBIT 5, the latest version of COBIT, has five major components; Structure, process descriptions, control objectives, maturity models and management guidelines. As a result, COBIT is used by organizations involved in business processes and related technologies and applies to the public and private sectors. The objectives of COBIT are the rapid exchange of information within the company to achieve business objectives through the integration of IT in strategy, minimization and control of company security information and risk management, IT optimization and cost of ISACA technology, and COBIT framework and research integration. Key principles include meeting stakeholder needs, ongoing corporate coverage, integrating multiple structures into a management transfer structure, and promoting a comprehensive business approach (White, 2017).

4. Cybersecurity breach case studies

The following case studies have presented previous examples that have occurred in various parts of the world with government organizations or other respected institutions around the world. Case studies have identified what happened on their respective sites and what measures are appropriate to deal with such violations in the future. The impact of these cyber security offenses highlighted the shortcomings of the information technology industry and provided insights that help to clearly understand the many gaps in the rapidly evolving technological world are cases related to security breaches of information found all over the world.

4.1. Saudi Aramco

This was considered one of the biggest attacks seen in the Middle East around the world. He was considered one of the best pirates in the world. The case occurred on August 15, 2012, in Saudi Arabia, considered one of the richest countries in the Middle East due to its large oil capacity and commercial activity (Pagliery, 2015). Due to oil activity in the country, many targets are often sought in the country to steal the country's revenue due to an increase in company resources. This allowed hackers to carry out their illegal activities at one of the world's largest oil companies, which would have the most negative impact on the country.

The company's computer network was affected by a virus that automatically replicated that it had infected more than 35,000 computers in a matter of hours, destroying all available Windows-based computers during that period (Pagliery, 2015). This has caused serious damage to the company, considered one of the company's largest oil and gas companies. Studies have shown that the recovery of damages in the business was so severe that it took almost two weeks to restore the total losses. It is clear that many cases usually occur in networks of different companies and that they usually have virus attacks. In this case, however, several attacks have resulted in a society so critical of the global energy sector and other oil markets in the region. Subsequently, the virus was identified while Shamoon was destroyed. This has caused a major disaster for the world's largest oil producer.

It was observed that the virus played an important role in the elimination of data from computer systems. This resulted in the loss of important information in a matter of hours without a trace (Pagliery, 2015). Although the Aramco virus has not caused any other unforeseen events, such as oil spills, explosions or other serious errors, many business processes have been seriously affected by the virus injection into the company's systems. The main problems observed as a result of the virus were the drilling of data and the injection of viruses seriously hampered other types of data production into computer systems. It has also been discovered that the Shamoon virus has spread to other companies in the country's energy sector, such as the Rasgas oil company.

Possible prevention measures

Protecting oil operations in Saudi Arabia due to physical attacks has become an important issue in recent years. Several steps would be appropriate to allow the company to ensure that this injury did not occur in the company's network. Oil confusion in the country has a major effect on the country and even in many parts of the world, as we have seen in this case. The company is responsible for the responsibilities and responsibilities assigned to all employees, especially those with good education sector education (Doell, 2012). This would detect injury for a while before the corporate network damage. The appropriate steps were taken within a period of time when the violations were discovered. The company also needed to use a powerful firewall on the Internet to investigate the attack (Doell, 2012). The firewall will also be updated by current trends based on the complexity of managed data.

Prevention strategies

The agency must ensure that web threats are well understood. This ensures that basic safety measures for all employees are possible so that appropriate action should be taken if there are any transactions in the system. The company should also ensure that it always works with the international security company to implement appropriate safety measures if necessary (Doell, 2012).

4.2. eBay Hack 2014

eBay is one of the world's leading e-commerce enterprises and offers several solutions to provide products and services available to all users around the world. The company has had many years of success in e-commerce all over the world until 2014, one of the world's greatest security breaks I have seen (Coty, 2014). The agency agreed to recognize the blow in business. This led to a significant loss of key customer and data losses that were difficult to recover after the disaster. Attacks were considered to be one of the most serious and dangerous attacks in the history of the world, which lasted for a long time without a well-known company.

These attacks were directed to user information and registrations, where users accessed more than 145 million registered users. These vendors were allowed to reach millions of records and steal all the searches an individual searched for without users having a basic awareness of the attack (Coty, 2014). The type of attack of these invaders was the attack on destruction and the use of social engineering. In this case, this attack was used to encourage users to use several tips, the user who wants to chat with the company's legal staff. This has resulted in sending their key features to their user accounts and details. As a result, insurgents were able to reach a network of 229 days. This is a long-term attack based on studies without a company having an awareness of violations. When the company understood the problem, these users had stolen many records.

Possible prevention measures

It was found that the wound had been lost for a long time ago, but studies have shown that the time spent on the attacker is very short, since it has taken him a long time to escape the information (Coty 2014). The company should take several measures to prevent the breach of the business. This will enable the company to recognize these characters for their incentives and, if necessary, warn their customers. The company will use all users and accounts, the password-end date technology, so it is advisable to temporarily change the password for the length and strength needed. The company had the technology to store more important information about external clients. Therefore, unauthorized access is not possible. It would be difficult for accountants to enter the systems and get important customer data when it happened. The company must also have used the filtering system to block the site's malware sites. It would also be difficult for employers to get lobsters to persuade users to report on their information.

Prevention strategies

The agency should consider various records relating to supervised customers. This is the main reason for hacktivist activity in the community. The company must be sure that illegitimate customers have no benefit at all (Doell, 2012). This will reduce the amount of risk that still appears when accessing customer records. The organization has to run the campaign to ensure that customers have never been told.

4.3. Ashley Madison Hack

The company provides network dating services and other social networks around the world. It turns out that the company was seriously affected by July 2015 when the company data breach exploded. The attack was carried out by a group of hacktivists known as The Impact Team. 40 MB of data was stolen on the company's website (Basu, 2015). Data included customer information and other internal Avid Life Media documents, as did in the refusal of computer systems. The Piracy Group has published several reports that have led the company to hide more than 30 million confidential information on the site. In August of the same year, the group published data on publishing data for nearly 37 million users of the company. This information contains confidential user information, including credit transactions and their phone numbers. Vendors continued to publish stolen data in August of the same year. In September, a group of hacker passwords reported that it had broken 11 million users of the company and ran further with its technology (Basu, 2015).

Possible prevention strategies

The company would have taken several steps to prevent it from avoiding it. The company should use network guidelines and social networks (Doell, 2012). This would avoid the rest of the internet network and social networks. Employees must also have received appropriate policy policies. The company should use, as well as security servers and security programs available, to prevent malicious software from attacking the computer and endangering unnecessary information.

Prevention strategies

The agency must report an increase in illegal activity, especially on the social media forum. This will help to employ all the necessary measures that ensure that appropriate security measures are being affected. Those who expect to use users must have permanent access to a closed site (Basu, 2015).

4.4. Under Armor

In 2018, Under Armor received data leaks in one of the most commonly used applications for MyFitnessPal applications. During the crime, accountants can steal 150 million personal information, including users' names, passwords and email addresses (Goud, 2018). Due to lack of security, arbitrators can receive and spy users' names and email addresses. Fortunately, passwords were saved by the most powerful algorithm (McGee, 2018). Fortunately, underground applications did not collect government ID and there was no chance of losing it. However, they collected information about a credit card or debit that was stored separately and never did. While still clearly important information such as credit card/debit credit cards, 150 million people and personally identifiable information have been placed in the right hands. This has a result. According to lawyer Steven Teppler, Abbott Law Group (which is not involved in the case), is it dangerous to email addresses, users' names and social engineering customers irritate, especially if It is expected that these data will be included. Spam key "(McGee, 2018).

After data violation, Under Armor was immediately rejected by shareholders. After the break, stock prices fell 3.9% (Aiello, 2018). There was recently an embarrassment on the fact that the companies did not agree with their claim and after the case. Group Media Information put in action "applicant, Rebecca Elizabeth Murray, MyFitnessPal user, complaint against Under Armor, including the breach of the contract, negligence, privacy violation and violation of several California law, is fair and misleading doing business.

Possible Prevention strategies

Some of the key features that come out are that the passwords were saved by the bcrypt event which was more difficult to delete and was not known, but email and user names used only SHA-1, which is easy to decrypt (McGee, 2018). Additionally, credit/debit cards were stored and used in different locations that were not covered. And if that's the case? Where did they get enough security using the bcrypt hash? None of these answers met with the investigation but should be dealt with. Under Arms should spend more time and money in the highest security possible for personal customer identity details. For a long time, this will save them from the lost money, actions, and attributes.

5. Major Prospective to Consider

Each organization must ensure that the appropriate information security system is selected. The organization's strategy should be aware of the needs and understand their needs to understand the required safety structure. The first point of view will be that "a separate view of IT agencies, including security and activity, as well as internal audit information on general requirements should be issued (Schlarman, 2007)". Another perspective to consider when selecting the correct information security structure is the organizational structure. Organizational structure affects the new structure and is it wise to have the same structure in the organization? The final perspective is how the structure will affect external factors. Many organizations work with partners and clients. One thing that the organization should consider is that this structure affects daily relationships with business partners and clients.

Other factors that can help the organization determine which organizational structure is most accurate is the overall cost, time, the convenience of effectiveness and effectiveness. The main purpose of many organizations is to produce profits. For this reason, the overall cost of implementing the information system is important. Cost is not just an important thing, but also a time limit. Organizations want a system that can be implemented quickly and efficiently. They want to provide their employees with the security they need to deal with existing regulations and procedures.

6. Computer security management in companies.

IT's risk hazards have been identified as special risks that, when considered more exercise, make it impossible to control the activity, often ignoring the outcome of the activity and connecting with other threats. Activity (Rigby, 2015).

To employ legitimate staff, regulatory and creative procedures, IT security must be controlled so that the branch is completely closed at the business level. Therefore, it must also be preserved as another risk of substances; The time has come to integrate IT security management into high-risk management (Rigby, 2015).

The growing dependence on information innovation and current public and private control systems covers the dangers of cyberbullying. Therefore, they must fear the various commercial risks and facilitate the risks for all management groups. While many leaders still regard digital security as a very specific problem that makes official government difficult, it is more important than ever for delayed memory. However, these tensions are linked to general risk management (Rigby, 2015).

Security risks related to the use of very powerful computers can be addressed in models that can be adequately managed by foreign governments or with oppressive mental links. Some use access to innovation for a guaranteed deposit, while others rely on external governments that seek to undermine national security and the economy. From time to time, intelligent writers can subtly introduce a structure and create the opportunity to travel over time without the revelation of a system in which information is downloaded for long periods in small steps.

A corporate risk management system offers greater legal and administrative guarantee (Rigby, 2015). However, this is not just a cure for cyber threats. The analysis of the risk probability of cyber-security is extremely problematic due to the limited information available in case of cybersecurity due to the episodes detected. They speak only of certain events that lead to specific vulnerabilities. The expansion will depend. When everything is ready, we can assume that the risk is 20% higher than what can be observed.

There are some types of IT security risk management that everyone can get through a company. Although no one is perfect, it reflects the differences between the organization, the number of trapped passengers and the cost of running an exposed administration (Rigby, 2015). Small and medium-sized businesses offer an excellent opportunity for a model that sees no difference between IT security management and operations.

7. Advantages and disadvantages

A broad outlook of the pros and cons of information security helps organizational leaders make better decisions about information security. Some of the benefits of information security management are to avoid risks. The lack of an information security system makes the organization vulnerable and potentially dangerous. Another specialist will ensure that

the appropriate controls are implemented to enable employees to be more aware of the threats and react to security breach situations. Other participants are tasked with helping the organization mitigate the costs. When an information security system is implemented, important information can be stored in a secure location, which can be costly for a company if the problem has been solved.

In his article "Design and validation of basic information on safety culture," Areej AlHogail states that: "Culture that promotes healthy human behavior in terms of safety through knowledge, devices, values , and assumptions of safety is much more effective than rules apply only to employees." From this excerpt, it is imperative that in all organization's employees are equipped with the necessary skills and are trained on precautionary measures to enable them to tackle any situations through knowledge of Information Security management framework. Also, employees should be trained on appropriate measures to maintain this structure.

Information security management offers not only advantages but also certain disadvantages. A major drawback is that threats are developed. As technology evolves, so do the threats to that technology. Unfortunately, information security management systems cannot be prepared without the proper knowledge of these threats.

8. Methodology

8.1 Type of Investigation

The study will use qualitative research methodology. The methodology is relevant because the qualitative research emphasizes the description of a scenario and meaning rather than the number, and thus the results of the qualitative research are descriptive rather than. Moreover, the researcher conducts the study by building a complex, holistic picture, analyzing words, reporting details of informants. The qualitative research provides a greater understanding of a concept or embodies a problem, rather than carrying out precise measurement or qualification. With the understanding from existing qualitative research, it has been declared that qualitative research needs to address the issue of philosophy (the ontological and epistemological assumption), methodology (clear steps) and the methods (the tools used for information gathering).

The use of a qualitative approach in this study will provide an inductive view of the relationship between theory and research. The study will start with a comparison between theories, theoretical issues which will then drive the formulation of a research question which will, in turn, drive the collection and analysis of data. After that, using findings will be fed back into the relevant theory.

The use of quality research in this study has some advantages. One is that the material can be investigated more accurately. There are often barriers to search methods. The purpose of the term limit is to create a test result to ensure that metrics can be used. Proper research focuses on the metrics of data collected and more on the trickiest points

that are not available. This allows a large amount of information, which allows you to collect more information during the test.

Another advantage is that the system can have water and depend on the input or existing data. In many research opportunities in a particular format of questions, data collection and you should follow. Quality research offers different ways. It can be adjusted for quality information collected. If data does not appear to show results, a search can convert the subject immediately and try collecting data in new addresses. This gives you more opportunity to find important information on a few topics, from small and regular perspective to achieving personal fulfilment.

8.2 Data Collection Method

Vital to any research study is the collection of relevant data, without it, researchers can't obtain desired results. In this quantitative research study, the methods that will be utilized to collect data will be through reviewing the relevant journals. Journals provide various data for the study. It is possible to get an array of information from the journals which have been peer reviewed. Websites will also be used to collect the data. The data will be analyzed and conclusions derived from the journals.

9. Research Limitations

Research data gathered by qualitative research can be time-consuming. The amount of data collected from quality surveys may be worse. You will be asked to take a temporary break of time. This is an independent effort, and that's why the researcher considers it important because it has not been removed from another researcher. At any time, the law may be neglected, the additional problem of the problem is much more difficult at a certain time.

Data quality is obtained thanks to the quality of production quality and the quality of the researcher's investigation. If you are still misleading the vision, it is possible to appear as part of the collected and affected results. Controls will be managed in their place to eliminate the risk at least so that you can gather them together. Otherwise, you specialize in research and research, conducting initial searches for quality research, for example, opinion perspectives.

10. Results

The Best Framework for an Information Security Office

Based on this study, the COBIT framework is the best framework for improving information security in an organization. According to IT Audit and Control Systems (2018), COBIT offers internationally recognized policies, practices, and tools that create trust in the company's IT system. Unlike ISO 27002 and NIST, COBIT covers a wide range of

organizational requirements, allowing the company to continue to focus on improving its strategies and achieving its goals (Haviluddin et al., 2012). The COBIT framework aims to optimize the organization's IT structure, which can be consistently implemented to ensure long-term goals. Gomesi Ribeiro (2009) emphasizes that COBIT has a direct impact on the company's performance, covering the operations and strategies of the company. Based on operations, COBIT helps organizations reduce their operational costs and increase their reliability, especially when they need IT for their daily tasks. Regarding strategies, COBIT guarantees the implementation of the correct procedures and support for success (Gomes i Ribeiro, 2009), since business opportunities often require IT support.

Omari (2016) emphasizes that COBIT effectively minimizes the risks associated with various organizational problems. These risks include security breaches, unreliable data integrity, inadequate spending and investment, information interruptions, service interruptions, and a lack of accountability. COBIT also promotes a better regulatory environment (Omari, 2016). With the growing impact of technology in today's world, regulatory requirements are increasing as users expect safe and reliable use of information technology. To this end, COBIT enables correct compliance and facilitates the implementation of an organization through the COBIT model.

Recommendations / improvements

Organizations that focus on the application of the COBIT framework should consider the following recommendations:

- Because COBIT encompasses a broad range of organizational security, organizations need to focus on processes of interest to improve their adaptability to the framework, to be proactive and non-responsive.
- The organization should focus on innovative goals, adapting COBIT to the main objectives.
- Also, organizations must ensure compliance with regulatory requirements and identify those responsible for the proper implementation of the structure.

11. Conclusion

The threats related to cybersecurity throughout the study have shown that threats within organizations need to be taken seriously. In most cases, companies end up losing data to hackers who end up using against the organizations resulting in millions of losses. It is therefore imperative that organizations take measures to curb these threats. Organizations also need to be aware of the growing threats to IT security and must perform reliable network operations and other access points on their technology devices in each location and location. The concrete cases eBay, Ashley-Madison, Under Armor and Saudi Aramco are one example. These companies and their customers suffered damages for an avoidable situation. Customers and the organization were exposed to fishing, fraud, and spam due to lack of preparation of the company. This could have been avoided if you had used the strong hash algorithm with usernames and email addresses. Organizations

of security organizations around the world should work more closely to ensure that they take the right measures at all times.

Information is one of the most valuable assets of an organization because it facilitates operations without commercial problems. Therefore, information security is essential to prevent unauthorized access to information and prevent the loss and corruption of information. Common organizations to ensure information security for organizations are ISO 27002, NIST and COBIT. According to the results of the survey, COBIT is the most appropriate structure for an information security office because its uses are very diverse since it focuses on IT and administration. However, further research is needed on the effectiveness of COBIT 5, since the previous study focused on earlier versions of COBIT.

References

Aiello, C. (2018, March 30). Under Armour says data breach affected about 150 million MyFitnessPal accounts. Retrieved September 27, 2018, from https://www.cnbc.com/2018/03/29/under-armour-stock-falls-after-company-admits-data-breach.html

Abagail, A. (2015, August). Design and Validation of Information Security Culture Framework. *Computers in Human Behavior, 49*, pp. 567-575.

Basu, E. (2015). *Forbes Welcome*. *Forbes.com*. Retrieved 28 December 2016, from http://www.forbes.com/sites/ericbasu/2015/10/26/cybersecurity-lessons-learned-from-the-ashley-madison-hack/#4539c09aed99

Chaeikar, S., Jafari, M., Therdoost, H., & Kar, N. (2012). Definitions and Criteria of CIA Security Triangle in Electronic Voting System. *International Journal of Advanced Computer Science and Information Technology*, *1*(1), 14-24. doi:2296-1739

Coty, S. (2014). *The eBay breach explained*. *www.scmagazine.com*. Retrieved 28 December 2016, from https://www.scmagazine.com/the-ebay-breach-explained/article/537762/2/

Doell, L. (2012). *10 Essential Cybersecurity Measures*. *OPEN Forum*. Retrieved 28 December 2016, from https://www.americanexpress.com/us/small-business/openforum/articles/10-essential-cybersecurity-measures/

Goud, N. (2018, March 30). Over 150 million users of MyFitnessPal affected by Cyber Attack. Retrieved September 27, 2018, from https://www.cybersecurity-insiders.com/over-150-million-users-of-myfitnesspal-affected-by-cyber-attack/

Gomes, R., & Rebeiro, J. (2009). The Main Benefits of COBIT in a High Public Educational Institution - A Case Study. *Pacific Asia Conference on Information Systems*, 1-11. Retrieved from http://aisel.aisnet.org/pacis2009/88

Haviluddin, H., Anthony, P., & Alfred, R. (2012). The Utilization of COBIT Framework Within It Governance: A Study of Literature. *The 2nd ACIKITA International Conference on Science and Technology (AICST)*, 1-8. doi:10.13140/2.1.3616.4160

McGee, M. (2018, June 1). Lawsuit Filed in Wake of Under Armour Data Breach. Retrieved September 27, 2018, from https://www.bankinfosecurity.com/lawsuit-filed-in-wake-under-armour-data-breach-a-11051

Omari, L. (2016). It Governance Evaluation: Adapting and Adopting The COBIT Framework for Public Sector Organizations (Ph.D.). The Queensland University of Technology.

Pagliery, J. (2015). *The inside story of the biggest hack in history*. *CNNMoney*. Retrieved 28 December 2016, from http://money.cnn.com/2015/08/05/technology/aramco-hack/

PECB. (2018). ISO/IEC 27002:2013 Information Technology - Security Techniques Code of Practice for Information Security Controls.

Rigby, J. (2015). *Cybersecurity and Risk Management: Lead from the C-suite*. *Legacy.alixpartners.com*. Retrieved 28 December 2016, from http://legacy.alixpartners.com/en/Publications/AllArticles/tabid/635/articleType/ArticleView/artcleId/1929/Cybersecurity-and-Risk-Management-Lead-from-the-C-suite.aspx#sthash.VyxzTPDI.dpbs

Schlarman, S. (2007, Feb). Selecting An IT Control Framework. *EDPACS*, pp. 11-17. Retrieved from http://search.proquest.com.ezproxy.trident.edu:2048/docview/234907576?pq-origsite=summon

U.S. Department of Commerce. (2018, November). Cybersecurity. Retrieved from https://www.nist.gov/topics/cybersecurity

Von Solms, R. (1998). Information security management (1): why information security is so important. *Information Management & Computer Security*, *6*(4), 174-177. doi:10.1108/eum0000000004533

White, S. (2017, December). What is COBIT? A framework for alignment and governance. Retrieved from https://www.cio.com/article/3243684/methodology-frameworks/what-is-cobit-a-framework-for-alignment-and-governance.html