Developing Cost-effective Cybersecurity Management System for Academic Institutions in Saudi Arabia

Talal Alharbi

Department of Information Technology, College of Computer and Information Sciences, Majmaah University, Al Majma'ah 11952, Saudi Arabia, talal@mu.edu.sa

Abstract

Technology in the recent years has dramatically invaded the education system and profoundly changed the classroom landscape, especially in modern universities. Internet of Things (IoT) devices, such as automated attendance tracker, interactive whiteboards, etc., are significantly utilized to create a positive and engaging classroom atmosphere. Unfortunately, some emerging universities deploy these smart tools before establishing an effective cybersecurity management system to protect critical characteristics of information, i.e., confidentiality, integrity and availability. The cybersecurity management system in academic institutions is the most-targeted system for cyberattacks, which is growing rapidly and hits businesses worldwide every day. To shed lights on the impact of this critical problem, we introduce a cybersecurity management system designed specifically for academic institutions based on Saudi Arabia. The paper also looks closely at the best practices and the adoption of international information security management standards deployed in worldwide academic institutions.

Keywords:

Cybersecurity ; risk management; information security; ISO; NIST

1. Introduction

The digital transformation we are witnessing nowadays has changed the nature of technology growth and expanded its utilization until the Internet has become a global means of everything in our lives. Most devices and appliances, such as security systems, thermostats, etc., are now equipped with additional features, creating a connected hub where information can be shared and exchanged between these physical devices and users over the Internet.

Cybersecurity attacks are growing rapidly around the globe due to the rise in the number of smart connected devices, i.e., IoT devices and the lack of information security awareness among the Internet users. Therefore, holding training session on security awareness and educating interested users discreetly are the key factors to prevent data breaches. As can be seen in Figure 1, which represents the top attack vectors reported in 2018 and 2019, Malware is observed as the most common attack vector used nowadays by cybercriminals because the users are not broadly aware of the risk and malware threats [1].

In addition, cyberwarfare has become the strategic war and new frontier of the information area, especially in countries with limited resources, where cyberwarfare capabilities are mainly developed to compensate for their deficiencies and shortcomings in sophisticated defense functions [2]. Figure 2 shows the cybersecurity threats and attack vectors being performed across a wide range of sectors even though some sectors, such as education are less attractive to the attackers. After the analysis of the data reported in [1], it is determined that the attacker behaviors have gradually changed over time.

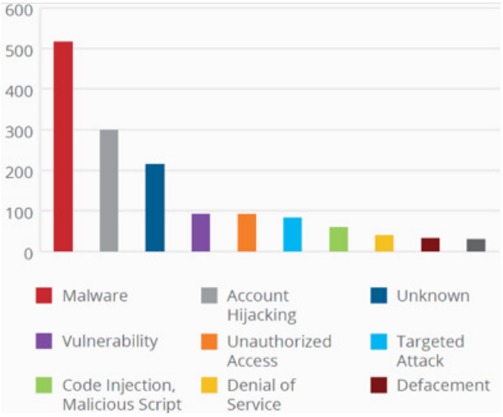

Fig. 1. Top Attacks Vectors Observed in 2018 and 2019 [1]

They have become interested in corrupting and damaging the information system of academic institutions as in other sectors where the main interest is financial gain. Academic institutions in general face two critical challenges to successfully achieve a secure environment. The first one is the amount of personal information held in the database system is enormous while there is no efficient and effective infrastructure, capable of delivering information security. The second one is that they are increasingly deploying different systems and technologies to satisfy diverse learners and meet their expectations, before having an effective cybersecurity management system in place and establishing security risk assessment.

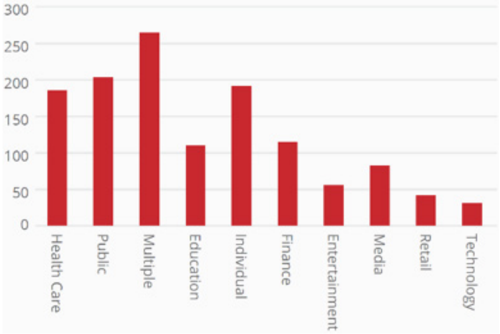

Fig. 2. Top Targeted Sectors Observed in 2018 and 2019 [1]

The adoption of cybersecurity management systems is quite low particularly in public organizations. This happens due to multiple reasons, such as shortage in the number of expertise, time to prepare required paperwork and no support and involvement from the top management [3] [4] [5]. Most of the academic institutions are applying well-known standards such ISO 27001, COBIT, etc., even though those standards are not purposely designed for higher education institutions [6]. In addition, the different regulations each country must locally comply with can make the implementation more challenging.

Therefore, the main motivation of this work to analyze cybersecurity management systems implemented in academic institutions and propose a new one designed specifically to fit the nature of educational organizations in general. The key contributions of the paper lie as follows:

- Investigating well-known frameworks designed for protecting sensitive data.
- Studying the key reasons that drives most Saudi universities away from adopting the best practice.

- Designing a Cybersecurity Management System (CMS) to govern data based on mix of ISO and NIST standard that meet the environment of Saudi universities.

The rest of the paper is structured as follows: Section 2 provides the relevant background on Information Security Management System (ISMS) and well-known standards. Section 3 presents related works and Section 4 describes the proposed implementation methodology for developing Cybersecurity Management System (CMS) for academic institutes in Saudi Arabia. Section 5 illustrates the proposed system in details and Section 6 discusses the benefit of the implementing CMS in academic institutions and, Section 7 concludes the paper.

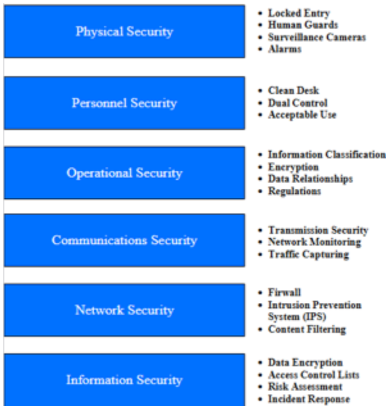

Fig. 3. Cybersecurity Layers

2. Background

2.1 Overview

Information is the lifeblood and vital business asset of any modern organization. It is essential for the business sustainability and continuity because accurate and up-to-date information would effectively help stakeholders in decision-making. The characteristics that form the value of information include availability, accuracy, authenticity, confidentiality and integrity. The value commonly increases and decreases based on changes happen in those characteristics [7], [8], [9].

Therefore, organizations need to have multiple layers of security simultaneously in place to protect its employees, clients, vendors and partners from harm. The harm can be intentionally committed by adversaries or unintentionally by insiders, violating the security procedures and practices being manipulated [9]. Figure 3 shows those security layers, which are described as follows:

- Physical security, which provides security for physical assets from unauthorized access.
- Personal security, which provides security for authorized individuals in the organization.
- Operation security, which is mainly designed to provide security for a particular operation and activities.
- Communications security, which is mainly designed to protect all communication media and data going through it.
- Network security, which is mainly designed to secure all network equipment and connections.
- Information security, which is mainly designed to preserve the confidentiality, integrity and availability of information in all stages: transmission, storage, or processing. This can be achieved via policies and security awareness and

training. The policies are the directive that establishes procedures and processes for organizations to protect information elements and critical assets, while the security awareness and training program is conducted by security experts and provided to the people to make sure they comply with legal requirements and technologies.

2.2 Cybersecurity and Information Security

It is important to note that the term cybersecurity and information security is often used interchangeably even though there is a conceptional distinction and overlaps each other. The International Organization for Standardization (ISO) defines information security as maintaining the confidentiality, integrity and availability of information. The National Institute of Standards and Technology (NIST) defines information security as preventing privacy, disruption, destruction and modification of information and systems to provide authorized users with confidentiality, integrity and availability. In [9], information security is defined as the maintenance of confidentiality, integrity and availability of information and all its elements such as the systems and hardware where information is used, stored and transmitted. Information security is essentially a set of practices mainly intended to prevent data from unauthorized access and mitigate the information risks.

Cybersecurity is a broad term that encompasses physical techniques, such as intrusion detection and prevention systems, firewalls, mantrap, ID cards, badges, etc., and logical techniques, such as best practices, safeguards and procedures to protect functions and cyber environment of an organization.

The concept is wider than information security, in which its core functionality ensures the attainment of all security objectives and prevents the entire cyberspace from cyberattacks [10]. To be more specific, cybersecurity includes large defensive methods utilized to minimize risk by detecting and thwarting sophisticated attacks before reaching an organization's cyberspace.

3. Related Works

Cybersecurity has recently caused considerable problems for most organizations especially when internet is the delivery medium. This fact is overlooked by organizations, in which they believe their information is valuable and sensitive, e.g., health, banks, etc. In contrast, in academic institutions, less papers have discussed the concern of information security even they often encounter the same type of threats and incidents happen usually in other sectors.

In [11], the authors develop a framework to evaluate the information security management systems and make sure the security strategy is aligned with other strategies, taking into their consideration all the information security aspects. The main problem here is that the authors did not include the low-level model that can guide any organization during the framework adoption. The paper [12] proposes a generic framework to improve the development process of the information security policy. The framework is high-level statements and does not include the details and the procedures to implement the requirements correctly, as we have done in our paper.

The authors of [13] review and assess the risk activity in the campus based on the risk predication technique. No framework is discussed in the paper even though the information is found to be at risk of exposure. The paper [14] addresses a strategic framework for information security management developed based on a systematic review and provides recommendations to higher education institutions to protect the information from security threats. Our paper is extended to cover all information aspects and provides an efficient framework developed specifically for Saudi Universities. The paper [15] proposes an information security management system for the academic institutes in Pakistan by introducing new roles and responsibilities. The new role introduced is Information Security Management-Task Force (ISM-TF), responsible for the methodologies and the processes for the system. The responsibilities of the Chief Information Security Officer (CISO), the Information Security Officer (ISO), the Internal Auditor, Network Administrator and System Administrator have been also extended to provide information security. However, this approach is not enough as the authors of [16] find out that knowledge and attitude are the key factor behind the success of the information security management system based on the investigation they did on the impact of organizational culture and behavior. Advanced technology tools alone are insufficient to provide confidentiality, integrity and availability to the information assets. There is a big need to focus on teaching employees to comply with the cybersecurity rules to make the information security management more effective.

In [17], the authors collect data from a Norwegian University through the Security Operations Center (SOC) department and investigated 550 cybersecurity incidents occurred between 2016 and 2017. The results show that most of the cybersecurity incidents happened due to successful social engineering attacks while the rest happened due to reconnaissance, intrusion attempt and denial of service. Figure 4 summarizes those cybersecurity incidents. Therefore, the system we proposed includes information security management and cover important cybersecurity domains. The aim is to reduce the implications of the data breach that are thoroughly discussed and addressed in [18], [19].

4. Methodology

The paper adopts the content analysis research technique that can find patterns and trends to develop a conceptual framework based on the results of analyzing most popular information security framework. We focus on those where largely adopted by Saudi academic institutions and then we explore the challenges and the issues that were obstacles to the implementation.

4.1 Information Security Challenges in Academic Institutions

Academic institutions generally face

unique cybersecurity challenges that can easily disrupt their ultimate goal of contributing to society and enriching lives of students through the pursuit of education and research. Meanwhile, academic institutions are often unable to support large scale security solutions, due to lack of funds even though critical information from students and staff has been stored into their systems. Thus, enforcing practical policies capable of governing collected information is quite problematic and sometimes impossible, especially when the top managements are not cooperative and supportive. For instance, the paper [20] explores the key reasons behind low adoption of international standards to manage information system in Saudi Arabia. Based on the investigation, we summarize the significant factors that affect the implementation of international information security management system standards as follows:

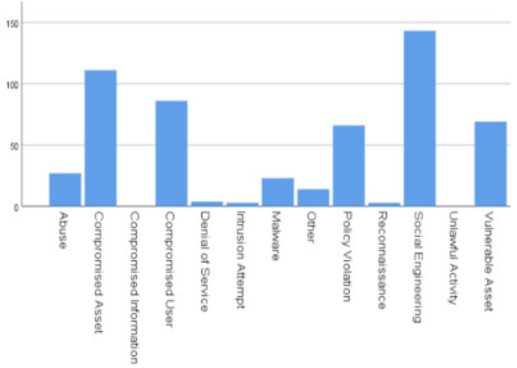

Fig. 4. The Main Causes of Cybersecurity Incidents in a Norwegian University [17]

- Lack of management support, direction and knowledge in most effective and well-known cybersecurity management system.
- Lack of funds allocated to support high salary required by security experts and perform training, education and awareness programs to the employees.
- Lack of resources and consultants who are professionally able to deal with international information security standards.

The other challenge with the Saudi universities is that some of them have multiple campuses exist in different places, which can be far away from the main campus, where the data center is physically located. Even with the single administration, the access privileges assigned to approved entities and the level of access are typically loose and difficult to control. Most importantly, there is no certain policy that clearly states the length of granted access and when the access should be given. This creates environmental concerns of placing critical information systems at risk and opening doors for those who are interested to access inappropriately [21].

Therefore, many academic institutions must consider cybersecurity as their top priority because cybercriminals are becoming a lot more complicated in executing attacks. This has increased the need to develop effective cybersecurity strategies meant to enhance security postures and prevent computer systems and networks from sophisticated cybersecurity threats. However, prior to that, it is important to understand current cybersecurity frameworks already established for the same purpose.

4.2 Cybersecurity Standards and Frameworks

For protecting and persevering information assets, specialized information security organizations, such as the National Institute of Standards and Technology (NIST), the International Organization for Standardization (ISO), the American Institute of Certified Public Accountants (AICPA), etc., have established comprehensive and rigorous methodologies and specifications to enhance information security. Despite their similarities and integration possibilities, there are differences in degrees of complexity, scale and the procedures for the management and mitigation of cybersecurity risk. Table 1 summarizes top cybersecurity frameworks in terms of the creators and key focuses while Table 2 discusses those frameworks in terms of their strengths and weaknesses as well as the organizations that the framework is suitable for.

Table 1. The Focus of International Information Management Standards

Cybersecurity Framework	Developed by	Focus
NIST	National Institute of Standards and Technology	Cybersecurity risk management and aligning cybersecurity posture to the core organization objectives
ISO IEC 27001	International Organization for Standardization	Cybersecurity management program
COBIT	Control Objectives for Information and Related Technologies	Aligning business objectives to IT objectives
HITRUST CSF	Health Information Trust Alliance	Providing approaches for enhancing security
HIPAA	Health Insurance Portability and Accountability Act	Protecting health information
CIS Top 20	The UK Department for Business, Innovation and Skills	Providing knowledge on the impact of cybersecurity issues
ITIL	Information Technology Infrastructure Library	Aligning IT services to the business needs
IASME Governance	UK cybersecurity business	Demonstrating the cybersecurity level
SOC 2	American Institute of Certified Public Accountants	Protecting data in cloud services
FedRAMP v7	Federal Risk and Authorization Management Program	Evaluating threats and risks in cloud-based infrastructure and software solutions
FISMA	Federal Information Systems Management Act	Providing security requirements

Cybersecurity Framework	Developed by	Focus
TC CYBER	Technical Committee on Cybersecurity	Improving privacy in telecommunication channels and media & Telecommunication organizations
GDPR	General Data Protection Regulation	Providing security requirements to enhance personally identifiable information

Table 2. Detailed Comparison of International Information Management Standards

Cybersecurity Framework	Strengths	Weaknesses	Fitting
NIST	Easy to adapt, flexible and freely available	Determining action items is difficult	Any organization
ISO IEC 27001	Widely implemented, Support various compliance requirements	No recent update and high cost to obtain and maintain	Any organization
COBIT	Control Objectives for Information and Related Technologies	Aligning business objectives to IT objectives	Any organization
HITRUST CSF	Comprehensive, flexible and support various compliance requirements	High cost to obtain and maintain	Mainly for health organizations
HIPAA	Easy to adapt, Flexible & Complex	High cost to obtain and maintain	Health organizations
CIS Top 20	Flexible and easy to deploy	Insufficient and updated every two years	Any organization
ITIL	Easy to adopt, flexible and efficient	Not suitable for a startup organization	Organization with IT function
IASME Governance	Affordable	Insufficient	Small and medium-sized organization
SOC 2	Support various compliance requirements	Need to be confirmed by vendors, not easy to deploy, high cost	Any organization
FedRAMP v7	Sufficient and comprehensive	Difficult to deal with and required experts	Government agencies
FISMA	Sufficient and comprehensive	Difficult to deal with and required experts	Federal agencies
TC CYBER	Flexible and comprehensive	High cost	Telecommunication organizations
GDPR	Flexible, continues improvement	Insufficient	Any organization

Even though some of the above standards and frameworks are widely used for Information Security Management System (ISMS), none of them focus on building ISMS for academic insinuations. Thus, from our prospective, establishing a Cybersecurity Management System (CMS) sometimes known as an Information Security Management System (ISMS) specifically for academic institutions is vital to achieve the goal of protecting their critical infrastructure and information against breaches and other incidents. It generally helps organizations, regardless of their size, degree of cybersecurity risk and cybersecurity sophistication, improving resilience and security through the implementation of effective policies and procedures and best security practices.

5. Cybersecurity Management System (CMS) for Academic Institutions

5.1 Overview

The CMS we propose basically describes the approach to managing information security and specifying the minimum requirements of security controls that academic institutions should implement aligning with their business needs to drive improvements in information security. The key elements we include in the proposed framework are:

- Appointing special staff with enough knowledge in the security field.
- Identifying the risks generally face the academic institutions in Saudi Arabia.
- Applying security solutions to mitigate the risks.
- Designing proper security policies based on the risks.
- Filling the risk register and tracking the progress.
- Training employees on the policies and examining awareness.

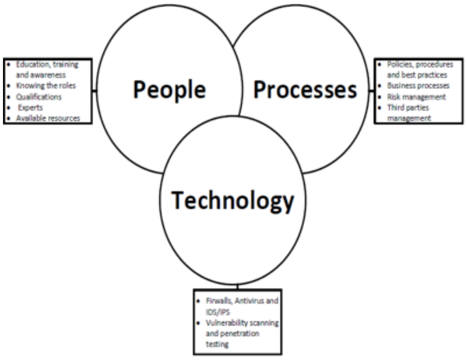
Education, training and awareness
Knowing the roles
Qualifications
Experts
Available resources
People
Processes
Policies, procedures and best practices
Business processes
Risk management
Third parties management
Technology
Firwalls, Antivirus and IDS/IPS
Vulnerability scanning and penetration testing

Fig. 5. Cybersecurity Pillars

The system formalizes processes and procedures for any expected vulnerabilities to make sure the perimeter of defense systems is protected. The common type of cyberattacks the system aims to defend against include Malware, Phishing, Man-in-the-middle, Denial-of-service, SQL injection, Zero-day exploit, DNS Tunneling and other more.

The system as shown in Figure 5 is comprehensive and includes the pillars of cybersecurity, i.e., people, processes and technology to manage all security practices consistently. It is impossible to deploy technology effectively without competent people, supporting processes and an overall plan. The system helps to determine whether the organization meets a whole range of compliance requirements in respect to information security and meet data security compliance obligations for several laws. Furthermore, the system is meant to help the organization achieve its objectives.

The key factors that drive the success of the proposed system are senior leadership commitment, top-down approach management and employee’s involvement. The top management team must rank cybersecurity as their top propriety and provide necessary resources and budget, so that the implementation team can deploy and maintain the system successfully. They must involve in setting cybersecurity strategies and understand that cybersecurity is an ongoing process. More importantly, this helps the board get better overview of security regime. The top management team must also believe that cybersecurity is applied to them so the staff in this case tends to take the same kind of view [22].

Another factor is the staff engagement, where everybody has a role to play in cybersecurity and must receive enough and continuous training, education and awareness about cybersecurity. However, the level and the depth of the cybersecurity education is not the same as the level the Chief Security Officer (CSO) training and IT manager receive. It is significantly less and generic that covers basic cybersecurity concepts and data privacy and governance. The main purpose of the staff awareness program is to be aware of wide range of cyber risks and gain basic knowledge of the best practice on how to achieve information security in an effective way and reduce preventable mistakes.

5.2 Proposed System

Prior to developing the system, a thorough research has been carried out and queried reliable databases for the following keywords: "cybersecurity system", "cybersecurity management", "cybersecurity in higher educations", "security framework in academic", "attacks on universities database", etc. The proposed system is designed based on the results of this review and the authors experience in the cybersecurity field and university management and administration. It is meant to be internationally certified by ISO/IEC27001 and established based on the execution guidelines described in ISO27002. The evaluation and certification criteria must be done based on ISO27001 through monitoring the execution over a certain period.

The goal is to govern critical information in the academic institutions in Saudi Arabia effectively and protect their assets from most common cybersecurity threat. It basically integrates some available cybersecurity frameworks and standards discussed previously to make sure the proposed system covers most important aspect of security through specific security controls, policies and procedures. The system covers technical and non-technical information issues.

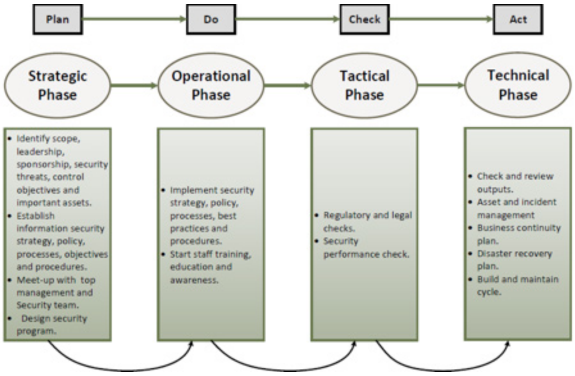
Plan
Do
Check
Act
Strategic Phase
Operational Phase
Tactical Phase
Technical Phase
• Identify scope, leadership, sponsorship, security threats, control objectives and important assets.
• Establish information security strategy, policy, processes, objectives and procedures.
• Meet-up with top management and Security team.
• Design security program.
• Implement security strategy, policy, processes, best practices and procedures.
• Start staff training, education and awareness.
• Regulatory and legal checks.
• Security performance check.
• Check and review outputs.
• Asset and incident management
• Business continuity plan.
• Disaster recovery plan.
• Build and maintain cycle.

Fig. 6. Cybersecurity Management System

We aim to make it comprehensive and include organizational, documentary and hardware and software components to overcome biggest threats, such as malicious software, phishing and social engineering. Problems might face the deployment of the proposed system that we must take into our consideration are:

- Budget and resources requirements.
- Regulatory compliance.
- Employees' behavior.
- Accurate security requirements.
- Exponential growth in the number of users.
- New technology integration.

5.3 System Elements

The implementation of the proposed system is divided into four essential phases: strategic, operational, tactical and technical. For the continual improvement and development, we associate the phases with the Plan Do Check Act (PCDA) cycle [23]. Figure 6 shows the elements of the CMS we mainly design for academic institutions in Saudi Arabia. In the following, we are discussing each phase in more details.

5.3.1 Strategic Phase

In this phase, a primary attention is given to the meeting with the top management, e.g., the president of the university, senior leaders, e.g., the dean and the vice dean of information technology deanship and security team, e.g., Chief Information Security Officer (CISO) and Information Security Officer (ISO). The engagement and commitment of the board is critical in this stage since they should provide accurate information for the following:

1. Top cybersecurity risks currently threaten the university.
2. The complexity of current infrastructure.
3. The budget that is allocated to increase the security posture.
4. The current plan for disaster recovery and data breach.
5. The compliance level with current cybersecurity controls.
6. Number of information security risk assessments conducted per year.
7. The risk posture, details of risks included the transition plan and the results of the gap analysis.
8. The information security frameworks and standards currently in place.
9. The object and attributes of desired measurement.
10. The visibility of the network and the procedures to test systems prior to problems arise.

The direction for information security must be set by the president of the university while the senior leaders are required to provide additional support to enforce board's directions and make information security everyone's responsibility. The problem that most Saudi universities face is the enforcement of the direction and policies, especially when the university has multiple branches far away from the main campus. Therefore, the major responsibilities of CISO will be extended to include the following:

- Designing and implementing cybersecurity strategies capable to prevent data and IT systems from well-known attacks [24].
- Setting up a business continuity plan for any new system and application along with a disaster recovery plan as a final step prior to go live.
- Influencing data governance and educating all parties involved in data processing, e.g., data owner, data steward, data producer and data consumer.
- Monitoring and evaluating end user' compliance toward information security controls and policies established by the university.
- Leading the communication channel among university employees, top management team and vendors.
- Conducting cybersecurity awareness program using emails, social media, workshops.
- Measuring the university progress through well-defined Key Performance Indicators (KPIs).

5.3.2 Operational Phase

The problem usually happens in large organizations is the resistance to change, which becomes more complicated especially when the top management underestimates security threats facing the organization. Sometimes, the management practice itself could be the reason behind achieving a higher level of security and data privacy in the universities [24].

Therefore, the CISO should appoint a Security Mentor (SM) in each campus, responsible for security awareness creation and delivery, backups, access management, data classification, key management and spreading the culture of security across the organization to make cyberthreats viewed as a business risk rather than an IT issue. This will bring more attention to any threats facing the university and make cybersecurity everyone's core business.

The SM is also responsible for applying security at the beginning of any activity since security becomes more complicated when the system is implemented. This can be achieved by holding multiple workshops and inclusive discussions with everyone, i.e., professors, employees and students within the campus where the SM resides. Followed by the creating the security operation plan that describes day-to-day activities. Then, the SM should implement the plan with help of CISO and everyone's in that campus. Compliance and performance should be monitored all the time and continually tested. Based on the findings, the SM should go back and review the plan and then report the final results with the CISO and other SM reside in other campuses. This is a critical step in the proposed CMS to maintain smooth operations and ensure there is alignment and integration between all campuses, which is very difficult to be pursued in midsize enterprises [25].

The benefits of this implementation include but are not limited to the following:

- Flexibility: Having SM in each campus will help the CISO make the implementation of the CMS across the university easy and smooth and align with other campuses to achieve the business objectives.

- Consistent Security Posture: The decentralization of some of the cybersecurity functions will assure the consistency of the security posture across the university and will help whenever there's an update on the security policies.

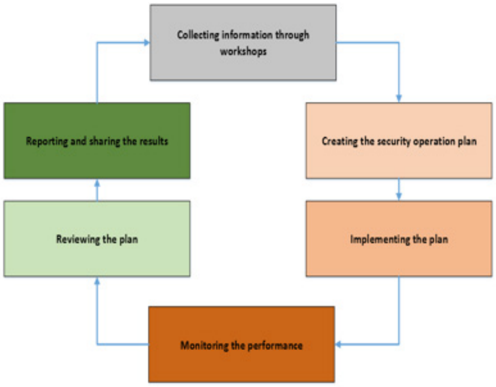
Collecting information through workshops
Creating the security operation plan
Implementing the plan
Monitoring the performance
Reviewing the plan
Reporting and sharing the results

Fig. 7. Cybersecurity Management Life Cycle

- Unlimited Support: When the CISO is directly reporting to the president of the university and the SM is directly reporting to the CISO, the support that each campus receives will be equal and endless.

Figure 7 briefly describes the life cycle of the proposed system, which starts by collecting information through multiple workshops with stakeholders and all the staff members of the organization. Then, the security operation plan should be established along with its own Key Performance Indicators (KPIs) to measure the plan in the future. After that, the CISO must proceed with the implementation of the plan and must track the progress on a daily basis to make sure all the campuses are following the same processes provided in the operation plan.

In the proposed CMS, the responsibilities of the CISO are being slightly modified to include the following:

- The CISO is required to establish the security risk management context along with the organizational and strategic contexts to identify the risks and conduct vulnerability and critically assessments.
- The CISO must obtain accurate information regarding what the consequences of the risk are and when they might be exposed.
- Based on the assessment and during the monitoring and review stage, the CISO
- should be able to decide the likelihood. Then, the risk is evaluated in terms of tolerance or acceptability to decide what the most suitable treatment is, i.e., avoid, accept, mitigate, transfer, or terminate.

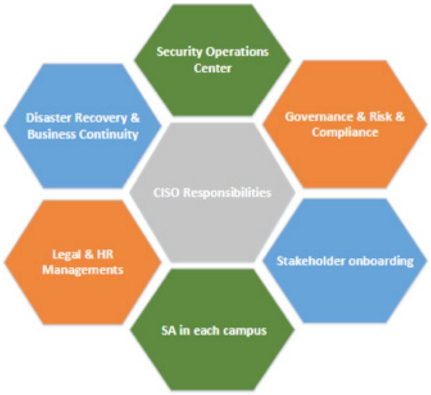
Security Operations Center
Disaster Recovery & Business Continuity
Governance & Risk & Compliance
CISO Responsibilities
Legal & HR Managements
Stakeholder onboarding
SA in each campus

Fig. 8. CISO Roles and Responsibilities

- The CISO is completely responsible for holding sessions between SMs and making sure the security maturity level is equal across all campuses. Figure 8 summarizes those responsibilities.

5.3.3 Tactical Phase

In this phase, the CISO should develop a comprehensive plan for recovering from data breaches, including recovery objectives, processes and procedures that ensure the critical IT systems and applications and other assets affected by future cyberattacks are restored in a timely manner. The plan should address all technical activity required to restore the core services as well as non-technical activity that affects the people and procedures.

The SM is responsible for identifying people, processes and technology assets that are necessary to achieve the university mission and then document the key personal who owns the data in the campus where the SM is currently at. This is critical to avoid messing with the data recovery procedures when there's an attack that needs immediate contact with the data owner to protect personal information from disclosure.

5.3.4 Technical Phase

The last part in this proposed CSM focus primarily on monitoring top information assets located in each campus, with their associated threats and vulnerabilities as described in Table 3.

To appropriately protect and manage the information assets hosted in the university, the SM should document all the details in the information assets register, which typically provides the following benefits:

Table 3. Security Risks Threaten Academic Institutions

Information Asset	Related Vulnerabilities	Related Threats
User credentials	Terminated employee	Gain access to the network, Credential lost and theft, User compromise
Personal data	Device lost or stolen, Malicious software	Gain access to the network and to sensitive business information, Ransomware
Information resources	Weak security controls	Unauthorized execution, Gain access to the environment
University data	Weak security controls	Disclosure, modification and destruction, poor data hygiene, poor data management and governance

- Making the maintenance much easier since the documentation is stored in a single location.
- Linking business requirements to information assets at an early stage.
- Managing risks that threat the assets.
- Controlling disposal and retention of the assets easily.
- Managing and monitoring accessibly, usability, responsibility and accountability.

The CISO should monitor and track the information assets register and prioritize them based on the critically and the severity using the following attributes:

- Asset name that should be meaningful.
- Description that summarizes the content and the function of the asset.

- User information that includes the creator owner
- Asset value that clearly defines the significance to the business.
- Asset lifecycle that addresses the retention rules and disposal action.
- Asset access that manages privileged users who have the right to update change, share and managed the asset.

These key attributes are the checklist that could be used for assessing the preliminary value of the information assets and determining the risk. The checklist could also be used during the most challenging phase, i.e., the information audit and quality assurance.

6. Discussion

The main problem with the academic institutions is that there are always limitations to apply an effective cybersecurity management system because the university in general is dedicated to educational and research purposes. Often, they do not focus on implementing or applying an effective cybersecurity management system while collecting the data. Therefore, the Cybersecurity Management System (CMS) proposed in this study is cost-effective and designed specifically for academic institutions to deliver safer and more trustworthy environment to host critical data. The system provides detailed procedures and clear roles and responsibilities that need to be followed. In this way, the system can identify threats, evaluate the current security controls, and then improve the design if required. The expected benefits after implementing the system include but not limited to:

- Reducing possible avenues of attacks and sensitive data exposure.
- Implementing consistent security controls across the organization.
- Allowing security and non-security experts for investigating and checking the compliance.
- Enhancing the cybersecurity posture inside the organization.
- Improving data governance and establishing data ownership.

The process for understanding the security threats existed in a system and determining the risks based on those threats is complicated especially when there is no solid CMS in place [26]. Therefore, it is highly recommended to have an effective CMS for academic institutions, willing to convert information security requirements into measurable and precise objectives, consistent across all campuses. This will help establish an appropriate mitigation for common attacks.

7. Conclusion

This paper lays down an effective Cybersecurity Management System (CMS) that should be implemented in most academic universities since information is critical from the time it is created until the time it is destroyed. The system provides the confidentiality, integrity and availability to the data and ensures the life cycle from a security perspective. The system should be regularly reviewed and updated even there is no change occurs to the business. This is a mandatory step to be able to separate between evil outside world and semi trusted inside.

The paper aims to provide a secure system, capable of protecting the most valuable asset the university owns, such as data from cyberattacks. The framework can also control diverse users with different levels of privilege. The system includes policy and procedures developed to ensure that cybersecurity in academic intuitions is successfully implemented. It also ensures the need for smooth and unhindered access to the information system is met since protecting and securing information resources is extremely crucial while given access privileges to users.

Conflict of Interest

None declared

References

[1] Beek, C., T. Dunton, J. Fokker, S. Grobman, T. Hux, T. Polzer, M. Rivero et al. "Mcafee labs threats report: August 2019." McAfee Labs, Aug. 2019.

[2] Eom, J. H., Kim, N. U., Kim, S. H., & Chung, T. M. (2012, June). Cyber military strategy for cyberspace superiority in cyber warfare. In Proceedings title: 2012 international conference on cyber security, cyber warfare and digital forensic (cybersec) (pp. 295-299). IEEE.

[3] Fomin, Vladislav V., H. Vries, and Yves Barlette. "ISO/IEC 27001 information systems security management standard: Exploring the reasons for low adoption." In Euromot 2008 conference, nice, france. 2008.

[4] Barlette, Yves, and Vladislav V. Fomin. "The adoption of information security management standards: A literature review." Information Resources Management: Concepts, Methodologies, Tools and Applications (2010): 69-90.

[5] Othman, Mohd Fairuz Iskandar, and Taizan Chan. "Barriers to formal IT governance practice--insights from a qualitative study." In 2013 46th Hawaii International Conference on System Sciences, pp. 4415-4424. IEEE, 2013.

[6] Alexei, A. (2021). Cyber security strategies for higher education institutions.

[7] Bishop, Matt. "What is computer security?." IEEE Security & Privacy 1, no. 1 (2003): 67-69.

[8] Tipton, Harold F., and Micki Krause. Information security management handbook. CRC press, 2007.

[9] Whitman, Michael E., and Herbert J. Mattord. Principles of information security. Cengage Learning, 2021.

[10] Von Solms, Rossouw, and Johan Van Niekerk. "From information security to cyber security." computers & security 38 (2013): 97-102.

[11] Leem, C. S., Kim, S., & Lee, H. J. (2005, September). Assessment methodology on maturity level of ISMS. In International Conference on Knowledge-Based and Intelligent Information and Engineering Systems (pp. 609-615). Springer, Berlin, Heidelberg.

[12] Ismail, W. B. W., Widyarto, S., Ahmad, R. A. T. R., & Abd Ghani, K. (2017,

September). A generic framework for information security policy development. In 2017 4th International Conference on Electrical Engineering, Computer Science and Informatics (EECSI) (pp. 1-6). IEEE.

[13] Awang, N., Xanthan, A., Samy, L. N., & Hassan, N. H. (2020). A review on risk assessment using risk prediction technique in campus network. International Journalof Advanced Trends in Computer Science and Engineering, 9(3).

[14] Merchan-Lima, J., Astudillo-Salinas, F., Tello-Oquendo, L., Sanchez, F., Lopez-Fonseca, G., & Quiroz, D. (2021). Information security management frameworks and strategies in higher education institutions: a systematic review. Annals of Telecommunications, 76(3), 255-270.

[15] Rehman, H., Masood, A., & Cheema, A. R. (2013, December). Information security management in academic institutes of Pakistan. In 2013 2nd National Conference on Information Assurance (NCIA) (pp. 47-51). IEEE.

[16] Ashenden, D. (2008). Information Security management: A human challenge?. Information security technical report, 13(4), 195-201.

[17] Wangen, G. (2019, June). Quantifying and analyzing information security risk from incident data. In International Workshop on Graphical Models for Security (pp. 129-154). Springer, Cham.

[18] Beaudin, K. (2015). College and university data breaches: Regulating higher education cybersecurity under state and federal law. JC & UL, 41, 657.

[19] Beaudin, K. (2017). The legal implications of storing student data: Preparing for and responding to data breaches. New Directions for Institutional Research, 2016(172), 37-48.

[20] Alshitri, Khalid I., and Abdulmohsen N. Abanumy. "Exploring the reasons behind the low ISO 27001 adoption in public organizations in Saudi Arabia." In 2014 International Conference on Information Science & Applications (ICISA), pp. 1-4. IEEE, 2014.

[21] Kurniawan, Endang, and Imam Riadi. "Security level analysis of academic information systems based on standard ISO 27002: 2003 using SSE-CMM." arXiv preprint arXiv:1802.03613 (2018).

[22] Abolhassan, Ferri. Cyber security. Simply. Make it happen. Springer, 2017.

[23] Kao, Yung-Wei, Chia-Feng Lin, Kun-Yao Cheng, Shyan-Ming Yuan, and Ching-Tsorng Tsai. "A PCDA-based critical exception management system in semiconductor industry." In 2010 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery, pp. 417-420. IEEE, 2010.

[24] Hansman, Simon, and Ray Hunt. "A taxonomy of network and computer attacks." Computers & Security 24, no. 1 (2005): 31-43.

[25] Otting, Jason H. "Factors Influencing the Adoption of Active Cybersecurity Measures Within Small to Midsize Enterprises: A Correlational Study." PhD diss.,

Capella University, 2020.

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