A Novel Security Framework to Mitigate and Avoid Unexpected Security Threats in Saudi Arabia

Ahmad Alshammari
Department of Computer Sciences, Faculty of Computing and Information Technology, Northern Border University, Saudi Arabia
ahmad.almkhaidsh@nbu.edu.sa (corresponding author)

Received: 5 June 2023 | Revised: 20 June 2023 | Accepted: 26 June 2023
Licensed under a CC-BY 4.0 license | Copyright (c) by the authors | DOI: https://doi.org/10.48084/etasr.6091

ABSTRACT
Many organizations around the world suffer large losses due to unexpected risks which can have a profound impact on their survival. This paper presents a novel security framework to address the security needs of Saudi organizations. There are four stages in the security framework: risk assessment and management, security intelligence and analytics, security policies and procedures, and security monitoring. A comprehensive security solution was provided by combining common security frameworks, e.g. ISO/IEC 27001:2013, NIST Cybersecurity Framework, and COBIT. The developed framework was designed to help Saudi organizations identify, assess, and control risks and respond to unexpected events in a timely and effective manner. It is expected to help organizations develop and implement effective security measures to protect their critical assets and operations from security threats. The proposed framework is comprehensive and can cover most organizations' requirements.

Keywords-security frameworks; security models; ISO/IEC 27001:2013; NIST cybersecurity framework; COBIT

I. INTRODUCTION
Many organizations experience a global revolution in governance that could affect how they manage their information. Organizations must ensure that their information is adequately protected and in compliance with information security laws [1]. A company's chief information officer should not only be responsible for securing data but also handle them as part of its governance practices. It is critical to note that corporate information security governance includes accountability to shareholders, compliance with legal requirements, setting well-planned security policies, spearheading security awareness and education, defining roles and responsibilities within an organization, establishing contingency plans, and implementing best practices [2]. The security of Saudi Arabian organizations is becoming increasingly important. The current challenges include a lack of emergency response plans that can lead to confusion and chaos during a crisis, poor risk management practices that can cause a company to be unprepared for a potential disaster, inadequate investment in cyber security infrastructure that can leave organizations vulnerable to cyberattacks, weak internal control systems that can leave organizations open to fraud and corruption, poor data protection and backup measures that can cause a company to lose important data in the event of a disaster, poor communication and collaboration between departments that can lead to delays in responding to an incident or event, insufficient training and awareness on emergency response procedures that can lead to mismanagement and errors, and inadequate insurance coverage that can leave a company exposed to financial losses due to an incident or event.

This study aims to develop a novel security framework using the Design Science Method (DSM) for Saudi organizations to avoid or mitigate expected incidents and risks. The proposed security framework embeds four stages, derived from existing security frameworks, such as ISO/IEC 27001:2013, NIST Cybersecurity Framework, and COBIT: risk assessment and management, security intelligence, security policies, and security monitoring. ISO/IEC 27001:2013 specifies the requirements for establishing, implementing, maintaining, and continuously improving Information Security Management Systems (ISMS) [3]. The NIST Cybersecurity Framework embeds 5 steps and translates the meaning of documents, such as ISO/IEC 27001:2013, into understandable information [4]. COBIT is an internal control structure of policies, procedures, and practices to provide organizational results and prevent, detect, and improve undesirable actions [5]. The proposed framework could enable Saudi organizations to better protect their data and systems and manage their security posture.

II. RELATED WORKS
Many studies addressed the security concerns of Saudi Arabian organizations and companies. In [6], various
cyberattacks in Saudi Arabia were examined, along with their effects, and solutions for a permanent solution to the problem were proposed. Cyberattacks were analyzed based on the type, source, extent, and type of information or service that was compromised. In [7], a model was presented to evaluate security risks. Essentially, it was a concept to understand and manage IT security risks comprehensively based on risk-based security management that incorporates organizational culture, knowledge, and security management. In [8], an information security policy compliance model was proposed that included variables such as resource weakness, self-efficiency, and awareness. According to the proposed model, security policy compliance is determined by three factors: self-efficiency, resource weakness, and awareness. The model suggested that when these three variables are high, compliance with security policies is more likely. Organizations should focus on increasing self-efficiency, reducing resource weakness, and increasing awareness to increase the likelihood of successful security policy compliance. In [9], a consistent framework was presented to measure the condition and suitability of the information security management frameworks of small and medium-sized organizations. However, small and medium-sized companies might not find it flexible enough to use it.

In [10], the role of secondary education in promoting information security among Saudi Arabian students was studied, as well as its realities, difficulties, and the necessary conditions for activation. The study discovered considerable discrepancies between men and women in what was needed to improve their culture. Secondary education was found to play a weak role in improving students’ attitudes toward information security, but first, the necessary prerequisites must be met. In [11], cloud attacks were studied among graduate students, discovering that most attacks were related to cloud storage security concerns. It was also noted that social networking security helps and creates awareness of the necessity of social awareness programs in higher education institutions. In [12], the perspectives of IT personnel in Saudi companies were investigated. Most of the companies studied had implemented information security policies and used ethical technology, but many of these policies were not properly and efficiently enforced or made public. The study encouraged the Saudi Communications and Information Technology Commission to create a national framework for instructing companies on ethical information security procedures. In [13], a model was developed to analyze the IS success model and cybersecurity elements that affect the efficiency and use of e-Gov services in Saudi Arabia. The findings showed that the basic IS constructs had a significant impact on the satisfaction of users and the degree of danger they perceived. In [14], cybersecurity was investigated from the Saudi Arabian e-Gov projects’ point of view, presenting a comprehensive approach that incorporated scientific principles. The study considered the operating environment of the project, focused on security, and claimed that cybersecurity must be developed and customized to meet the needs of citizens served by an e-Gov system.

In [15], a Cybersecurity Maturity Assessment Framework (SCMAF) was proposed for HEIs in Saudi Arabia, which was a comprehensive and customized security maturity assessment framework that can be used as a self-assessment method to establish security levels and highlight weaknesses and mitigation plans. SCMAF was implemented as a lightweight assessment tool that can be provided online or offline to ensure data privacy. In [16], the amount of data lost or stolen during data breaches was determined and the effectiveness of cybersecurity policies was investigated in companies. Multiple regression tests were used to evaluate the effectiveness of 12 cybersecurity practices in three areas for small businesses: financial loss, loss of sensitive data, and restoration time. In [17], the applicability of a theory-based model and the determinants of Information Security Compliance Behaviors (ISCB) among healthcare professionals in Saudi Arabian government hospitals were identified. The findings implied that while demographic traits have little effect on ISCB, moderating and uncommon factors, such as religion and morality, do. In [18], difficulties and impediments in security, privacy, reliability, integration, and data portability were examined in the health and patient care industries. Privacy and security issues with cloud computing and electronic health were discussed, as well as potential methods for dealing with them [19]. In [20], the security of different web applications was evaluated using a hybrid Fuzzy Analytical Hierarchy Process-Technique for Order of Preference by Similarity to Ideal Solution (Fuzzy AHP-TOPSIS) method. The study suggested integrating security in-between web application development. In [21], the present methods of the GCC countries for managing e-waste were reviewed, projecting the output until 2040 and covering the potential long-term effects on the economy, security, and ecology, suggesting steps to protect private data contained in discarded electronic components. The study recommended a thorough review of current legislation to address potential security and environmental challenges and emphasize economic opportunities.

Additionally, several studies aimed at discovering the risks for organizations. Organizations can use these studies to classify and respond to security events, mitigate risks, and expand their overall security attitude with the help of digital forensics. Numerous studies investigated and discovered incidents, data breaches, and other digital attacks on organizations [22-61]. As a result, the above review shows that Saudi Arabian organizations lack a comprehensive security framework to mitigate and avert possible risks, leading to a difficult situation in terms of monitoring, managing, and protecting all assets and resources of the organization.

III. METHODOLOGY

This study used DSM to develop a new security framework for Saudi organizations to mitigate and avoid unexpected events. DSM uses a combination of research methods to develop and test design solutions [62-63]. According to design science, research can solve design problems and improve products, services, and systems. The development process involves five steps:

- Identifying the problem
- Creating research questions
- Conducting an e-litterature review
- Developing a novel security framework
Investigating and validating the framework

A. Identifying the Problem

The purpose of this step is to identify the current problems that Saudi organizations face in the event of unexpected events or incidents. Assets may be destroyed or compromised due to such incidents. Several Saudi organizations are currently experiencing problems that may be affected by unexpected events, including the absence of disaster response plans, insufficient investment in cybersecurity, weak interior controls, lack of communication between sectors, and inadequate training and understanding of emergency response procedures.

B. Creating Research Questions

This step determines the research questions to identify the limitations and drawbacks of traditional security models for Saudi organizations. The research questions were "What security measures should Saudi organizations implement to protect confidential data and reduce the risk of data breaches?", "How do Saudi organizations protect their data?", and "What are their limitations with the existing security models?"

C. E-Literature Review

This step involved research on current security models and frameworks used by Saudi organizations. The search results included only articles published in journals and conferences between 2015 and 2023 in English. This period was selected because it ensured the availability of sufficient data. Table I summarizes the search results. The articles were filtered according to the research objectives. For this purpose, inclusion/exclusion criteria were selected. Based on the analysis of the security models and frameworks discovered, the development of a novel security framework was required to mitigate and avoid unexpected events. The proposed security framework should provide an integrated approach to security risk management, be comprehensive, and include components such as threat analysis, risk assessment, incident response, and security monitoring.

<table>
<thead>
<tr>
<th>Search Engines</th>
<th>Keywords</th>
<th>Results</th>
</tr>
</thead>
<tbody>
<tr>
<td>IEEE Explorer</td>
<td>Security frameworks, Security models, Saudi organizations</td>
<td>108</td>
</tr>
<tr>
<td>Scopus</td>
<td>Security frameworks, Security models, Saudi organizations</td>
<td>1010</td>
</tr>
<tr>
<td>Springer</td>
<td>Security frameworks, Security models, Saudi organizations</td>
<td>95</td>
</tr>
<tr>
<td>Web of Science</td>
<td>Security frameworks, Security models, Saudi organizations</td>
<td>1503</td>
</tr>
</tbody>
</table>

D. Developing A Novel Security Framework

The proposed security framework for Saudi organizations consists of five steps, as shown in Figure 1: risk assessment and management, security intelligence and analysis, security policies and procedures, and security monitoring. The developed framework was based on ISO/IEC 27001:2013, NIST Cybersecurity Framework, COBIT, and the SANS Top 20 Critical Security Controls.

1) Risk Assessment and Management Stage

A process that threatens a company's earnings and capital should be identified, assessed, and controlled. This stage involves identifying potential risks, assessing their likelihood and impact, and implementing measures to reduce risks to an acceptable level. An organization's operations would not be complete without it. This minimizes the risk of unexpected losses and maximizes the success potential of the organization. In addition, it helps to comply with applicable laws. Processes, operations, and products are analyzed for potential weaknesses or vulnerabilities. Assessing risk involves determining the likelihood of an event occurring and its impact on the organization. In addition to quantitative methods, qualitative methods, such as interviews and surveys, can also be used. As a third step, develop strategies that can involve changing processes and procedures, implementing new technologies, or insurance policies. Lastly, the organization should monitor and review its strategies over time to ensure their effectiveness.
Security Intelligence and Analytics Stage

In this stage, information is collected, analyzed, and interpreted. Organizations can detect and respond to potential threats with a detailed understanding of their security posture. This stage consists of several steps. First, collect and analyze data from a variety of sources, such as networks, endpoints, applications, databases, and cloud services. Second, automated threat detection using advanced algorithms and machine learning techniques. It is necessary to develop and implement a threat response and restoration plan to resolve the issue. Third, incident response and forensics, in which evidence is collected and analyzed to determine the cause and scope of a security incident. Fourth, risk and compliance management helps organizations identify, assess, mitigate, and comply with applicable laws and regulations. The final step is to protect information assets through security operations.

Security Policies and Procedures

Organizations can develop and implement security policies and procedures tailored to their specific needs and objectives to protect information systems, networks, and other assets from risks. Four components make up this stage: First, the development of security policies helps organizations protect their assets, data, and systems, as they provide guidelines to define acceptable use of technology. The second step is to implement security procedures to ensure compliance with security policies. Authentication systems, access control systems, and encryption techniques are examples of technical controls. In the third step, security logs, reports, and user activities are reviewed and audited regularly to ensure that policies and procedures are followed and that security incidents are handled appropriately. In the final step, employees must be trained and made aware of security policies and procedures, as well as provided with resources to make them aware of risks and vulnerabilities. Security-related training and awareness campaigns should be provided regularly.

Security Monitoring Stage

This step aims to regularly evaluate an organization's networks, systems, and applications to ensure that there are no vulnerabilities or malicious activity present. Monitoring an organization's IT environment continuously for suspicious or harmful behavior involves continuously observing and analyzing its activities. There are eight components in this stage. First, security event logging and analysis collects and analyzes logs from various sources, such as network traffic, applications, and systems, to detect anomalies or suspicious behaviors. The second step is intrusion prevention and detection which detects and blocks malicious traffic. Third, vulnerability scanning identifies and mitigates any potential threats by regularly scanning the network for known vulnerabilities. In the fourth step, it is ensured that all assets are secure, including hardware and software. In the fifth step, network monitoring is used to detect suspicious or malicious activity. In the sixth step, endpoint security is installed and monitored on all devices to protect them from malware or malware-like attacks. The seventh step involves user access controls, which establish policies to control access to resources by ensuring that they have the necessary permissions. Finally, security auditing is performed to identify any security vulnerabilities in systems and networks.

Testing and Validating the Framework

The developed framework must be tested and validated to ensure its capacity and effectiveness before using it in a simulated environment. Security experts and the organization should also evaluate and validate the framework's effectiveness. Future work will implement this step.

IV. DISCUSSION

The proposed framework includes four stages: risk assessment and management, security intelligence and analytics, security policies and procedures, and security monitoring. Organizations must identify, assess, and mitigate potential risks during the risk assessment and management stage. This stage identifies potential vulnerabilities and threats, assesses their likelihood, and develops and implements security measures to mitigate them. Data must be collected and analyzed to determine potential vulnerabilities and threats. Machine learning and artificial intelligence technologies can be used to detect anomalies by monitoring network activity and analyzing user behaviors. Developing and implementing security policies and procedures that protect the organization from potential threats and vulnerabilities is the goal of the policy and procedures stage. This stage also includes policies for access control, user authentication, and encryption. Lastly, security monitoring involves monitoring any suspicious activity within the organization's systems. Monitoring user behavior and reviewing access control policies are some of the steps involved in this stage. The proposed security framework provides a comprehensive approach to protect the organization from potential threats and vulnerabilities. As part of the security process, the organization's systems are monitored for suspicious activity and identified, assessed, and mitigated risks. This security framework was developed using ISO/IEC 27001:2013, the NIST Cybersecurity Framework, and COBIT, which are three common security frameworks. The proposed model may also work with organizations in other countries than Saudi Arabia, as it is built based on these common security frameworks. For instance, risk assessment and management are provided by the NIST framework, security intelligence and analytics are provided by the COBIT framework, and ISO / IEC 27001:2013 was used for developing security policies and procedures.

V. CONCLUSION

This study proposed a security framework for Saudi organizations to mitigate and avoid unexpected security events. The proposed framework was based on ISO/IEC 27001:2013, the NIST Cybersecurity Framework, and COBIT, and included four stages: risk assessment and management, security intelligence and analysis, security policies and procedures, and security monitoring. The proposed framework can also be applied in organizations of other countries, as it is based on three common security frameworks.

REFERENCES


