Cyber Security Governance Framework

Student’s Name

Institutional Affiliation

Cyber Security Governance Framework

**INTRODUCTION**

National Institute of Standards Technology (NIST) is a framework of cybersecurity that has been implemented by over 29% of organizations. The framework comprises standards, guidelines, and best practices to manage cybersecurity threats and risks. Additionally, NIST is a charitable framework whose primary intention is to help serious infrastructure organizations mitigate and manage cybersecurity risk based on the prevailing standards, practices, and guidelines (Bartsch & Frey, 2018). Notably, this cybersecurity framework has demonstrated flexibility so that non-critical and non-infrastructural organizations can also apply it. This paper aims to discuss how the National Institute of Standards Technology can improve cybersecurity management.

**BACKGROUND**

NIST was initiated in the year 1901 and is currently part of the US commerce department. From the records, NIST among the oldest laboratories of physical science (Bartsch and Frey 2018). The main aim of establishing the agency was to eliminate a core challenge to US industrial competitiveness in that error. It was a number two rate insulated behind Germany's abilities, the United Kingdom, and several other economic rivals. Notably, ranging from the smart electric power grid to atomic looks, advanced nanomaterials and chips of computer, services, and innumerable products depend in some way on technology, standards, and measurements given by the National Institute of Standards and Technology. NIST's primary mission is to ensure US industrial and innovation competitiveness by making the scientific measurement, technology, and standards in methods that promote economic security and improve quality of life. NIST achieves its mission via several programs.

Understandably, cyber threats and risk management is an essential concept of cybersecurity. In this case, the NIST framework and its application are known for improving critical infrastructure cybersecurity. With NIST, organizations provide recommendations and best practices that organizations can adopt to enhance cloud and internet security. Ideally, the framework provides a comprehensive framework of information security guidance for how an organization can access and improve its capacity to prevent and respond to cyber threats. Arguably, the NIST framework is organized into five essential functions: identity, protect, detect, respond, and recover. Each of these functions is well defined on how it can be implemented to mitigate possible cyberattacks and threats.

**CYBERSECURITY GRC IN SAUDI ARABIA**

Notably, cybersecurity Governance (GRC) in Saudi Arabia requires implementing a security risk assessment methodology and process. Additionally, GRC and in line with the NIST framework, enables organizations to achieve and address uncertainties relating to cyberattacks and risks reliably. Ideally, governance makes sure that an organization or a company has adequate administrative controls to ensure that all the risks were mitigated. Analysis of risks in this case also helps ensure that an organization correctly identifies, mitigates, and analyzes the risks. According to Prince and King (2012), it is notable that for several organizations and companies, it's the most crucial untouchable asset they have is their information. Therefore, it is very detrimental to make sure that they protect it. Notably, information security has significant roles in any organization or any company: It ensures that the functioning ability of the organization is protected, It ensures that the technology applied by the organization is safeguarded, ensures protection of the data collected and used by the organization and lastly, it facilitates the safe operations of the implemented applications on the Systems of IT relating to the organization.

The NCA and SAMA are Saudi Arabia entities of government that are basically in charge of cybersecurity and function as the national authority on all affairs relating to Saudi Arabia. NCA holds both the operational and regulatory functions that are connected to cybersecurity. It closely does its work with both public and private entities to ensure the improvement of the cybersecurity posture of the Saudi Arabia nation to safeguard its vital interests, the security of the country, critical infrastructures, high priority sectors, and also the services and activities given by the government in alignment with the set vision 2030.

In Saudi Arabia, the NIST GRC framework is structured based on four critical domains as follows:

1. Third-party cybersecurity
2. Cybersecurity Technology and Operations
3. Cybersecurity Governance and Leadership
4. Cybersecurity Risk Compliance and Management.

For every single domain, several subdomains are defined. The fundamental purpose of a subdomain is to focus on a particular topic on cybersecurity. Per every single subdomain, a principle, control considerations, and objectives are stated by the framework. According to Al-Sheikh (2017), a principle summarizes the critical set of preferred cybersecurity controls relating to the subdomain. The objective functions to describe the importance of the principle and what needed cybersecurity controls are expected to attain. Lastly, the control considerations in Saudi Arabia reflect the mandated controls of cybersecurity that must be put into considerations. Ideally, the control considerations have been numbered differently and uniquely all along with the framework. The need is that the control considerations can be made up of up to about four various levels. Below is a figure that demonstrates the overall structure of the framework in Saudi Arabia and indicates the cybersecurity subdomains and domains involving a reference to the applicable section of the said framework?

The framework is based on a principle which is also termed as risk-based. Ideally, it recommends the core cybersecurity principles and objectives to be achieved and embedded by the member organization. The listed control considerations, which are mandated, provide different directions, and must always be confirmed by the member Organization in attaining the objectives. When a particular control consideration can't be adapted or even applied, the member organization should all the time think about compensating controls, undertaking an internal acceptance risk, and appealing a formal waiver from SAMA.

**CURRENT PROBLEM**

As far as cybercrimes are concerned, Saudi Arabia remains to be the most renowned target. This is partly attributed to it being a significant oil source, but it is still because of its strategic location in an area with extensive tensions relating to geopolitics. In reference to IDC'S most recent survey by CIO, which was conducted in Saudi Arabia, Over 60% of CIOs in Saudi Arabia perceive security management as the most formidable challenge of technology, which is ongoing.

In the ministry of interior in Saudi Arabia, several different government websites were compromised via repeated cyber-attacks coming from outside the KSA. As a result, the websites were all rendered unworking for a short duration until the responsible organization was able to thwart the attacks (Shen 2014). Still, the National industrial Company (TASNEE), a petrochemical owned by an individual in Saudi Arabia, was affected by a cyber-attack. The attack destroyed all the hard disks of all the computers within a few minutes of inception.

Considering the current cybersecurity problem in Saudi Arabia National Institute of Standards Technology can properly aid in implementing the most beneficial cybersecurity practices. Considering the NIST's standards and the enforcement action posted by FTC's, a few guidelines happens to be the perfect practices of cybersecurity:

 Security. The framework advice on not gathering individual details that the organization does not need. Instead, any organization should always get focused only on the information only if it has any need that is very legitimate to the business relating to the business or the organization. Personal information must not be used when there is no need to do so. Any organization using this framework should always make it compulsory on appropriate security standards where its contract is needed; it should also ensure the verification of compliance, including via audits of cybersecurity provided by a third party.

**Identify**. This framework requires the company or any organization to properly understand its computer systems and its network, the individual information it gathers, possible challenges of the organization's systems, and the magnitude of harm that its clients are likely to experience disclosing their data.

**Protect**. The NIST framework requires that the organization develop and implement extraordinary measures to guarantee serious infrastructure services.

**Detect**. Through the NIST framework, the organization is always able to respond and implement the key activities to use relating to a cybersecurity event that is detected within the organization's systems.

**Recover**. NIST framework can always help implement best cybersecurity practices that can aid developing and implementing the best activities to ensure plans of resilience are maintained and help restore any services that could most probably be affected due to the incident of cybersecurity.

**CURRENT GRC BASICS, MODELS, FRAMEWORKS, AND VARIATIONS**

To reduce cybercrimes in Saudi Arabia and also security threats, three essential methods have been proposed as the solution: physical security, organizational awareness, policies and also training of the employees and thirdly technical measures of prevention.

Following the evolution of digital transformation strategies and the moving of industry undercurrents in Saudi Arabia, organizations are making organizations bring forth innovations and come up with new technologies and delivery models. As a result, this moves to create a more turgid ecosystem that is commonly affected by new cybersecurity challenges. Consequentially, cybersecurity in Saudi Arabia is no more limited to the protection of technology assets, but it also has the mandate to ensure the business's resilience. As far as the current framework is concerned in Saudi Arabia, it shows that the current community has higher aspirations relating to the customer's flawless experience, un lacking availability of services, and also fruiting protection of the critical data. Both online services and information assets are currently strategically significant to private and public organizations, including society. The said services happen to be crucial to making a digitally vibrant economy. They are still proving to become systematically significant to the nation's economy and its complete security.

**PROPOSED SOLUTION, MODELS AND FRAMEWORKS, AND ITS FEASIBILITY/APPLICABILITY**

Following the cyber threats in Saudi Arabia, a few solutions have been recommended to curb the threats. Firstly, to boost security and secure the cloud, the country's selection can significantly help. The data security is many times pegged on the exact location of the data center. For example, if the country or region is prone to terrorist attacks, such areas will automatically have data security issues. Secondly, an organization or a company should always ensure that all subscriptions are from an accredited cloud provider. Several providers of the cloud have been claiming that they always offer maximum security.

 However, it cannot win the subscribing organization or company's trust until it is fully certified by the third party. To confirm the security offering's offering, either the major or the minor providers of the clouds must be accredited to different standards to reflect the security level tabled by them. To ensure data security, selecting a reputable and accredited cloud provider functions is a significant and inevitable role. I brief, as a solution, it is very significant for the organizations and companies always to confirm the accreditation of the person or organization providing the cloud to certain specific standards. As a solution to personal data, organizations in Saudi Arabia should always provide and implement cybersecurity governance in line with NIST or any other cybersecurity framework to ensure identification, protection, detection, and recovery from cybersecurity risks.

**EXPERIMENT TESTING AND ANALYSIS**

The current society heavily depends on mobile devices whose hardware and software security is turning to be a global concern due to the increased number of daily attacks that are disclosed. The current cryptography methods for handling issues relating to security remain to be entirely unknown to the adversary. However, making sure that the simple concept is applied turns out to be very difficult because software such as Trojan horses and malware practiced by enemies with one access to a device can disclose the key, resulting in a security breach. The second difficulty comes from the fact that the PUFs are complex and very sensitive to input conditions. When conversion methods that are analog-digital are implemented for crucial generations, its sensibility can come up with different keys similar to input conditions.

The difficulty is in the impossibility of reproduction of the same conditions of input in various experiments. In a chaotic system that is strong, for example, PUF, even a little variation in the parameters of input can heavily affect the reliability of security primitive. SA is a material made up of an ultra porous network relating to silica aggregates, which are sparse. SA optical response is adjustable from complete transparency to chaotic scattering by controlling the inclusions of silica distributions and size by either optical or mechanical effects. As a result of the low thermal conductivity, SA exhibits a significant substantial opt thermal nonlinearity, mostly connected to large and reversible deformations of structure, thus resulting in nonlinear controllable material that can randomly be implemented in various fields of applications.

In conclusion, applying a cybersecurity governance framework provides a roadmap for improving risks associated with cyberattacks. This report has addressed the NIST framework, which provides cybersecurity governance, paying attention to five critical functions, including identifying, protecting, detecting, responding, and recovering.

References

Al-Sheikh, A. (2017). Cyber Security Framework Saudi Arabian Monetary Authority. Saudi Arabian Monetary Authority.

Bartsch, M., & Frey, S. (2018). Cybersecurity Best Practices. Springer Fachmedien Wiesbaden.

Prince, D., & King, N. (2012). Small Business Cyber Security Survey 2012.

Shen, L. (2014). The NIST cybersecurity framework: Overview and potential impacts. SciTech Lawyer, 10(4), 16.

Singh, A. (2020). CyberStrong: A Primer on Cyber Risk Management for Business Managers. Sage Publications Pvt. Limited.