CYBERSECURITY: PANORAMA AND IMPLEMENTATION IN 2021

ADEL I. G. IBRAHIM
RMG, Kingdom of Saudi Arabia

ABSTRACT

Cyber threats have changed the universe of enterprise security. These threats are often difficult to determine and locate particularly in the digital and mobile era. Cybercriminals behind these threats possess knowledge, intelligence, creativity, flexibility, and resilience, which increase with time. Security measures taken to mitigate these threats require the cooperation of multiple security disciplines, because a single discipline cannot address the issues of growing threats. This paper first presents the panorama of cybersecurity and its components; subsequently, it reviews the cybersecurity landscape in terms of various frameworks, models, and recommendations issued from specialized organizations and institutions such as NIST, ISO, CSI, and ISACA. This paper attempts to guide enterprises to navigate this supercharged landscape as well as to implement a sound cybersecurity model that is suitable for a specified industry and situation. A methodology was developed in this study. The methodology recommends a framework that is based on a cross section of standard frameworks but adapted to the levels of decision making in the enterprise. The proposed methodology was applied to an institution in the public sector, whereby the cybersecurity panorama was explored, and the best practices suitable for the activity and the processes of the institution were implemented. Thus, a project with defined phases was executed. The methodology also suggests a sense of continuity, as cybersecurity is a never-ending endeavour.

Keywords: cybersecurity, cybercrime, malicious software, cybersecurity standards, cybersecurity frameworks, NIST 800, CIS controls, cybersecurity governance, cybersecurity strategy, cybersecurity implementation.

1 INTRODUCTION

In the 21st century, almost all companies use some type of digital systems (at least email, which implies internet access) and, therefore, are vulnerable to cyber-attacks because their data are not protected. Information breaks occur on a practically regular basis, uncovering email addresses, passwords, credit card details, and other exceptionally sensitive information.

Several users do not comprehend the severity of the issue until it "bites" them. Individuals and organizations alike are attacked fraudulently, usually by experts.

A credit scoring company, Experian, has published statistics for late 2020, showing that 31% of stolen personal information led to complete identity thefts.

Data theft in companies are more subtle, as the effect of cyber breach can manifest itself few months after the occurrence of the breach, rarely or never noticeable immediately to address the issues.

Published lists of confidential customers' data or R&D top-secret product development data on the dark web are disastrous for the companies' operations.

Living with the discomfort of these information leaks has apparently become an inescapable fact presently. One significant approach for handling these leaks is to prepare for cybersecurity.

The preparation for cybersecurity is a construct that includes policies, some hardware, software, and an awareness of personnel.

The next few sections describe some notable incidents that occurred in 2020/2021, followed by discussions of the most common cyber threat. Subsequently, widely used

WIT Transactions on The Built Environment, Vol 206, © 2021 WIT Press
www.witpress.com, ISSN 1743-3509 (on-line)
doi:10.2495/SAFE210041

standards are discussed, followed by a description of a methodology that is currently being applied.

2 CYBERSECURITY INCIDENTS

An internet search can reveal the information of some major cybersecurity breaches. Table 1 summarizes some of the notable cybersecurity breaches in 2020/2021.

Table 1: Notable cybersecurity breaches 2020/2021.

#	Company	Date discovered	Damage	Exposed
1	Channel Nine (Australian broadcaster)	28/3/2021	• broadcast • internet • publishing	Inability to broadcast news and shows, no internet access, publishing tools down
2	Harris Federation	3/2021	Ransomware attack	Voluntary shut down, disabling accesses to email and coursework for 37,000 students
3	CNA Financial (cyber insurance)	21/3/2021	Ransomware attack	Voluntary shut down for three days, disrupting operations for customers and employees
4	Florida water system	11/2/2021	Poisoning water supply	Increase in the amount of sodium hydroxide to a potentially dangerous level, from 100 ppm to 110,000 ppm
5	Bombardier (airplane manufacturer)	2/2021	Compromise of confidential data	Compromise of the confidential data of suppliers, customers. and around 130 employees located in Costa Rica
6	Facebook (social media)	3/4/2021	533 million users exposed	Phone numbers, DOB, locations, past locations, full name, and in some cases, email addresses
7	One Class (online learning)	29/6/2020	Over 1 million	Students' full names, email addresses, schools/universities, phone numbers, account details, and school enrolment details
8	BlueKai (web usage tracking data (for marketing))	19/6/2020	Over 2 billion entries	Names, residential addresses, email addresses, and other identifiable data including web browsing activity
9	Postbank (financial institution)	14/6/2020	At least 8 million	8–10 million beneficiaries who receive social grants
10	Keepnet (security company)	9/6/2020	5 billion	*(Second breach in a few months)*
11	CPA Canada (Professional Association)	4/6/2020	329,000	Members' data
12	Truecaller (caller id service in India)	27/5/2020	47.5 million	Phone numbers, service providers, names, genders, and more information
13	Pentagon hacking	3/6/2021	Undisclosed	Thousands of emails

Note: The list is not exhaustive. For further information, see [1]–[3].

3 CYBERSECURITY RISK TYPES AND ANSWERS

The risks on information and communications technology (ICT) operation stem from two main threats:

1. Sabotage: Sabotage refers to an internal human resource problem to be resolved by human resources practices. There exist few reports in the literature on this issue [4]. The best safeguards are in the Human Resource Policy proposed by ISO 27001 but still cannot fully guard from cyber threats, even if they are thoroughly implemented. companies must trust their employees up to a certain extent and ensure that their backup procedure is sound and diversified.
2. Internet: The internet is considered a window to the world, and it is the most dangerous window that is open to hackers and other cyber criminals.

3.1 Cybersecurity threats

Cybersecurity threats can be classified into several categories as summarized in Table 2.

Table 2: Main cybersecurity threats.

#	**Type of cybersecurity threat**	**Description**
1	Distributed denial of service (DDOS)	Denying access to bona fide users by bombarding the resource that they want to access, to the extent that the resource stops functioning (the hammer technique).
2	Man in the middle (MitM)	Attack targeting a user that remotely accesses a server, which is implemented by intercepting the communication and mimicking the bona fide user to steal their credentials and sensitive information. It can also be used to confuse the user by returning different responses.
3	Malware and spyware	A series of attacks that penetrate the system and install themselves to monitor user activity and steal confidential data and any other malicious intent.
4	Advanced persistent threat (APT)	This sophisticated attack stems from gaining unauthorized access to a system and remaining undetected for a period of time to exfiltrate sensitive data.
5	Password attacks	Gaining access to the password of a bona fide user either by knowledge, educated guesses, or brute force.
6	Social engineering	This threat attacks the weakest links in a network – human targets.

Social engineering attacks are targeted toward normal users, who are lured to perform a seemingly inoffensive action – business as usual – that triggers a chain reaction of offensive results planned by hackers. The social security attacks are so common that they deserve a further development, as summarized in Table 3, for which the data are taken from PA Knowledge [5] and Zielinski [6]. Software and appliances products that are mainly associated to firewalls can be used, but the safe solution to address most of these threats is to make users aware so that they practice caution.

Table 3: Social engineering attacks [5], [6].

#	Type of social engineering attack	Description
1	Phishing	Sending fraudulent emails from a seemingly official source, asking to click on a link that introduces the hacker's malicious program (usually providing the hacker a backdoor access to data and operations).
2	Homograph	A user accesses a fake website that seems to have a genuine URL and then submits sensitive information on this website.
3	Trojan virus	A user downloads a file either from a fake website or from an email attachment that will create a backdoor that can be used by the attackers.
4	Ransomware	When introduced, it prevents a user from accessing the user system and data unless a ransom is paid.
5	Malvertising or adware	Online advertising; when opened, it introduces the hacker's programs.
6	Wiper malware	When introduced in a target system, it wipes systems and data.
7	Drive by download	Hacking genuine websites, inserting malicious software that will be installed in the device of the website user.
8	Rogue security	A software that warns a user of the presence of a virus on their device. The user genuinely believes it and submits financial information to pay for the removal of viruses.

3.2 Usual software for handling the security risks

The cybersecurity industry is thriving, and the developers of many products in the market claim that the products address many of the cybersecurity risks. Some products are almost necessary, and some are purchased depending on the budget of companies and the sensitivity of their systems. Table 4 lists the features of some of these software.

3.3 Policies and procedures

Software deployment is insufficient to handle cybersecurity. A set of policies and procedures related to the discipline of the manpower should be implemented. Most frameworks (described in the next section) recommend a set of these policies.

4 CYBERSECURITY FRAMEWORKS (STANDARDS)

Various organizations – associations, standards, and institutes – have developed frameworks for cybersecurity. These frameworks are a set of documentation policies or procedures that state the best practices for handling cybersecurity in any entity. They need to be applied, and, if the standard (e.g. ISO) has a certificate, evidence must be provided for certification that these best practices are implemented in the entity.

These frameworks are usually based on access control, audit and accountability, awareness and training, cloud services safeguards, configuration management, continuous vulnerability management, email browser and web services protection, identification and

Table 4: List of software used to counter cyber threat [7].

#	Software	Function
1	Penetration testing	Known as ethical hacking, whereby a hacker tries to penetrate a system externally and prepares a report on its vulnerability from the outside.
2	Vulnerability assessment	This software allows to identify (from the inside) possible penetration points.
3	Assets management	An inventory of all information assets (usually classified as well); these assets are servers, network devices, databases, and people.
4	Patch management software (includes bug fixing and security patches)	Software vendors usually discover bugs and potential security vulnerabilities in their software and prepare patches to be distributed to their clients, in order to plug the security gap or bug fix. This software manages and deploys these patches.
5	Configuration hardening	Some associations propose the best configuration for a piece of software (operating system, database, etc.). Cybersecurity personnel implement these recommendations and harden the configurations.
6	Multifactor authentication	This software allows for a second personal authentication for the user in addition to a password; the most common is a one-time passcode (OTP) on an individual's cell phone.
7	Data leakage system	This software allows to encrypt any item of data to circulate in the network so that it can only be seen by a recipient who has the decryption; any other person cannot read it in clear.
8	Security information and event management (SIEM)	The organizations install a security operating centre (SOC) whose main objective is to identify any attack (event) and raise an alarm.
9	User and entity behaviour analytics (UEBA)	The software creates a baseline of user behaviour using avant-garde techniques such as machine learning. It alerts when there is a change in behaviour, which implies that a different user may have gained access.
10	Security orchestration automation and response (SOAR)	These series of software automate and save the workflow and human intervention for the first time when responding to a cybersecurity attack, so that it is triggered automatically in the case of a recurrence of the same attack without human intervention.
11	File integrity monitoring	This software checks that any software (apart from data) has been unchanged or officially changed.
12	Intrusion detection system/ intrusion prevention system (IDS/IPS)	Mainly a feature in the firewalls, allowing the detection of known signatures of a cybersecurity attack and preventing the packet to go through.

Table 4: Continued.

#	Software	Function
13	Network access control	This software allows for setting a policy (who can access, which device can access, etc.) for accessing the network. It repudiates any other attempt of access outside the set policy.
14	Network detection and response (NDR)	This software allows for monitoring the traffic for malicious actions and suspicious behaviour and react in response to network threats.
15	Applications whitelisting	An index of allowed applications and software scripts to be run in a system. It does not allow for running any other application, thus limiting access to potentially harmful applications.
16	Endpoint detection and response	This software allows for detecting and responding to malicious activity on endpoint devices as well as responding to some such threats. It shortens the response time of security teams.
17	Malware protection	Malware = malicious software; types are viruses, worms, Trojan horses, spyware, malvertising, and ransomware.
18	Data encryption – standing data	Encryption of records or specific fields in a database so that it is accessible only to persons having the decryption keys.
19	Data encryption – transmitted data	Encrypts the network traffic to guard from "sniffing" the traffic.

authentication, incident response management, malware protection, media protection, monitoring of cyber-attacks, patch management, personnel security, physical and environmental protection, penetration testing, system and communications protection, and system and information integrity.

Two types of standards (frameworks) are used for cybersecurity [8]:

- Specific industry/trade/sector cybersecurity standards/frameworks.
- Generic or universal cybersecurity standards that are applicable anywhere.

4.1 Specific industry/trade/sector cybersecurity standards

These standards are developed by specific industries and sectors; they include many features that cover the operations of the sector. They are built based on a set of compliance requirements or cybersecurity controls that must be adhered to in order to be compliant and/or accredited.

4.1.1 Health Insurance Portability and Accountability Act (HIPAA), 1996 [9]

As the name suggests, this act is applicable in the medical field, banning the disclosure of patients' medical data without the consent of the person. The standard developed contains 64 compliance requirements and is applicable to all health providers: medical institutions (hospitals, clinics, nursing homes, pharmacies, etc.), professionals (doctors, psychologists, dentists, chiropractors, etc.), and medical insurance plans (insurance companies or employers). These health providers all need to be HIPAA-compliant by applying strict rules

pertaining to the confidentiality, integrity, and privacy of electronically protected health information (e-PHI) when it is created, stored, received, updated, or transmitted via electronic channels. It is mainly applicable in the USA but has a wider applicability in the Medical Profession.

4.1.2 Payment Card Industry – Data Security Standard (PCI-DSS) [10]
PCI-DSS is a security framework aimed at safeguarding cardholders' data when they use credit, debit, and cash cards. It is aimed at financial institutions, merchants, and individuals who create, use, transmit, accept, and honour payment with any such cards. It has 245 compliance requirements. It can lead to a PCI certification after a thorough audit. It is a worldwide standard championed by credit/debit cards companies such as Visa and Mastercard.

4.1.3 SOC 2 [11]
SOC 2 is a framework applicable to ICT service companies or software as a service (SaaS) companies. It safeguards customer data when they are uploaded into a cloud. It has 61 compliance requirements to ensure that organizations can control the privacy and security of customer and client data. It is an auditing procedure developed by the American Institute of CPAs (AICPA) and is based on a trust principle.

4.1.4 Others

- EU General Data Protection Regulation (GDPR) was effective from 25 May, 2018.
- It is an EU regulation with 98 compliance requirements to protect the personal data and privacy of EU citizens during transactions occurring within EU member states.
- NIST 800-53 is a framework developed by the National Institute of Standards in the USA (NIST), specific to the federal information systems, with 931 compliance requirements.
- NIST 800-171 lays out information security guidelines for the Department of Defense (DoD), USA. It is a subset of NIST 800-53.

Note: NIST has developed guidelines for specific purposes as above, but it has also developed a general guideline, NIST CSF (Cybersecurity Framework), which is described below.

4.2 General cybersecurity standards

These standards are to be used by any organization irrespective of its sector or trade from the government to SMEs or academic institution; they are applicable in any sector.

4.2.1 NIST CSF National Institute of Standards Cybersecurity Framework [12]
NIST CSF is one of the most popular frameworks in the world, and many national frameworks follow its recommendations. Fig. 1 shows its features.

NIST CSF has 108 subcategories of cybersecurity outcomes and controls, leading to 23 categories covered by the five functions shown in Fig. 1, which are applicable to all types of entities.

4.2.2 ISO/IEC 27001 [13]
ISO/IEC 27001 is an international standard to manage information security; it is published jointly by the International Organization for Standardization and the International

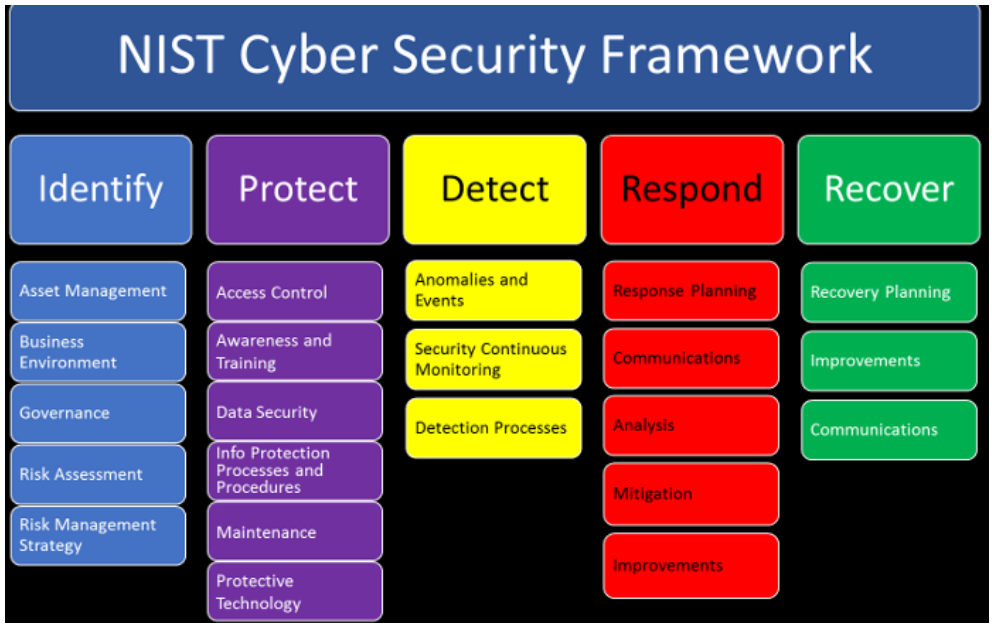

Figure 1: NIST Cybersecurity Framework. *(Source: Security Affairs.co.)*

Electrotechnical Commission. It has 114 compliance requirements for entities of any size in any sector. The standard is used for developing an information security management system and has an Annexure A for a series of policies and procedures. It has been widely applied across the world except in the USA.

4.2.3 CIS V8 Critical Security Controls (CSC) [14]

CIS V8 Critical Security Controls (CSC) refers to a framework developed by the Center of Internet Security. Fig. 2 shows the top 18 of these controls. The CSCs contain 153 safeguards. The CIS had divided the application of the standard according to the maturity level in implementation groups (IGs) orders from simple to the most complicated. These IGs are as follows:

- IG1 is called hygiene (to denote entry-level), having 56 cyber defence safeguards against the most common threats. It can be implemented by normal Information technology persons.
- IG2 refers to an intermediate level, having 74 additional safeguards, built upon the ones in IG1 but needs specialists (cybersecurity dedicated specialist) for implementation.
- IG3 refers to the expertise level and contains 23 additional safeguards to the above 45 and 74. This level requires experts for implementation. It caters to repel attacks by a sophisticated adversary.

5 WHAT TO DO: METHODOLOGY

The following points are extracted from all the frameworks mentioned above, and the methodology is proposed to adopt them in an organized manner by implementing a group of policies detailed in Fig. 3, whereby every block represents a policy containing the set of directives aimed to fulfil its purpose.

Figure 2: Top 18 security controls of CIS v8.

The methodology can be implemented through two groups within the organization:

- The leadership group, which is concerned with the strategy, governance, training, and definition of the responsibilities. These tasks are performed by a committee, which is composed of senior managers in the business units and the CTO, to oversee and monitor changes and advances over time. The committee can be called the ICT governance committee because it is responsible for the strategic direction of ICT services.
- The CIO group is concerned with operational aspects, policies and third-party relationships. This group is composed of the ICT hierarchy and relevant contracts management group (from purchasing). For protection, this group is responsible for identifying and acquiring the necessary software and tools performing the ICT protection. Budget is obtained and negotiated with the governance committee.

Fig. 3 illustrates the basic methodology as a framework.

5.1 Cybersecurity leadership

5.1.1 Cybersecurity governance

The organization must define a cybersecurity strategy, risk management framework, structured processes, roles and responsibilities, and top management oversight.

5.1.2 Cybersecurity strategy

The organization must define, document, approve, and implement a cybersecurity strategy, including the various initiatives, projects, programs, and references to internal and external relevant stakeholders. It should ensure reaching the desired and targeted cybersecurity maturity level with an alignment of objectives across all sectors.

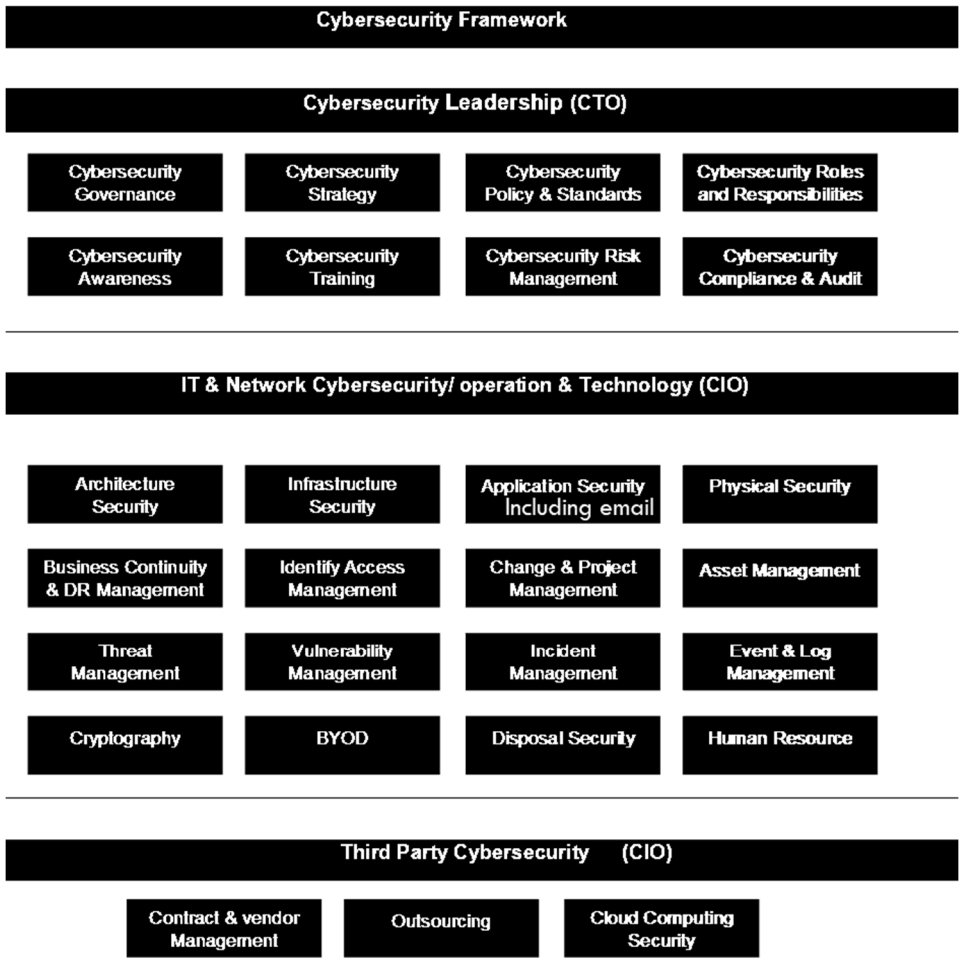

Figure 3: Methodology components.

5.1.3 Cybersecurity policies and standards

The organization must define, document, approve, implement, and communicate a set of cybersecurity policies and standards applicable to the organization setups and digital footprint.

5.1.4 Cybersecurity roles and responsibilities

The organization must define, document, approve, and implement roles and responsibilities within the context of the organization. These definitions shall be communicated to ensure that all relevant personnel and stakeholders understand their roles and responsibilities within the framework of cybersecurity.

5.1.5 Cybersecurity awareness

This topic concerns all organization's employees. It entails training (by presentation, film, pamphlets, placard, pop up screens, etc.), focusing on how employees gather knowledge

about cyber threats that they may face, and ensuring safety of the organization while employees fulfil their responsibilities.

5.1.6 Cybersecurity training
This topic concerns ICT professionals. It entails providing regular training to develop ICT employees' skills related to dealing with potential cyber threats, as well as to protect the organization's ICT assets.

5.1.7 Cybersecurity risk management
The organization must define, document, approve, implement, and communicate its risk management process. Cybersecurity risks are primarily focused on protecting the confidentiality, integrity, and availability of data stored, transmitted, or processed by ICT systems. It also ensures integration with the organization's enterprise risk management (ERM) and other relevant business processes.

5.1.8 Cybersecurity compliance and audit
The organization must establish a cybersecurity compliance process to periodically perform audits based on cybersecurity policies, legal and regulatory requirements, and industry standards or certifications (ISO/IEC 27001, PCI DSS, HIPAA, etc.) in order to identify, evaluate, manage, communicate, and monitor cybersecurity compliance. It should report its findings and any cybersecurity critical compliance violations needing the attention of the top management.

5.2 IT network, cybersecurity operations, and technology

5.2.1 Architecture security
Security requirements, standards, and controls are developed and defined based on the business requirements and criticality. The architecture is defined and documented according to the functionalities and security requirements described above. It is periodically reviewed and amended.

5.2.2 Infrastructure security
The organization must define, document, approve, and implement infrastructure security requirements and controls while periodically adjusting, monitoring, and evaluating its compliance to meet all security requirements, standards, and controls for infrastructure (external communication, endpoint devices, operating systems, database, servers, virtual devices, network devices, security devices, and file sharing).

5.2.3 Application security
Security controls should be applied for the development, procurement, and/or acquisition of an application, including mobile applications, Web services, and APIs, to ensure the secure closure of known gaps in the application, which can be exploited. These gaps might increase the risk of the organization.

A special application that should be monitored carefully is the email server; emails should also be monitored because they are used by everyone in the organization.

5.2.4 Physical security
Physical and environmental security measures are essential to prevent unauthorized physical access, damage and interference to the information assets, and information processing facilities.

5.2.5 Change and project management
The organization must define, document, approve, and implement change and project management requirements and controls that are incorporated and integrated into all stages of a project lifecycle' it should accordingly change management processes. Cybersecurity personnel are monitoring the project phases to ensure compliance. All the changes/projects must be tested in a test environment before implementation in the production environment.

5.2.6 Assets management
The asset management process starts at acquisition, followed by recording (register) with ownership, and finally classification and labelling. The management process then follows the stewardship of the asset throughout its lifecycle until disposal.

5.2.7 Business continuity and disaster recovery (DR) management
This framework is based on a business impact analysis study and the availability of a DR centre and an alternative work area. It is generally guided by the ISO 22301.

5.2.8 Identify access management
The organization must establish security controls to ensure the protection of information systems and data against unauthorized access, while still providing access to users who have a business need. It allows for various methods to authenticate genuine users and adopt stringent authentication processes for privileged users.

5.2.9 Threat management
The organization must define, prepare, approve, implement, and document a threat management process to describe a factual background for understanding the risks, early warnings, breach prevention, detection, and remediation efforts.

5.2.10 Vulnerability management
The organization must ensure timely identification and effective mitigation of application and infrastructure vulnerabilities to reduce the likelihood of incidents and business impact on the organization.

5.2.11 Incident management
The organization must define, approve, and implement a cybersecurity incident management to ensure the timely identification and handling of cybersecurity incidents, in order to reduce the (potential) business impact and to allow timely recovery from cybersecurity incidents. Disaster recovery plans include different scenarios of cybersecurity incidents.

5.2.12 Event and log management
The organization should define, approve, and implement a security event management process to analyse operational and security loggings as well as respond to security events. It should ensure timely identification of threats and respond to anomalies or suspicious events, particularly with regard to information assets.

5.2.13 Cryptography
Whenever needed, a cryptographic security standard should be defined, approved, and implemented. It usually covers data at rest, data transmitted over third-party communication lines, and the encryption of sensitive data when transmitted inside the infrastructure.

5.2.14 Bring your own device (BYOD)
Whenever the organization allows the use of personal devices (e.g., smartphones, tablets, laptops, etc.) for business purposes, their use should be supported by a defined, approved, and implemented cybersecurity standard in addition to staff agreements and cybersecurity user-awareness training.

5.2.15 Safe disposal security
The organization must dispose of its information assets safely when they are no longer needed. Thus, it can ensure the safety of its business, customers, and sensitive information from unauthorized disclosure upon disposal.

5.2.16 Human resources security
Human resources security is the weakest link in cybersecurity. Organizations should incorporate cybersecurity requirements into human resources processes. This will help ensure that staff cybersecurity responsibilities are included in staff agreements and that the staff are screened before their employment and made aware during their employment.

5.3 Third-party cybersecurity

5.3.1 Contract and vendor management
The organization must set up, define, approve, implement, and monitor the required cybersecurity controls within the contract and vendor management processes. This will help ensure that its approved cybersecurity requirements are appropriately addressed before signing contracts and that the compliance with the established cybersecurity requirements is being monitored and evaluated during the contract duration.

5.3.2 Outsourcing
The organization must define, set up, implement, and monitor the required cybersecurity controls within outsourcing policy and outsourcing process to ensure that its cybersecurity requirements are appropriately addressed before, during, and after exiting outsourcing contracts.

5.3.3 Cloud computing security
This framework is used to address the organization's use of cloud hosting services whenever applicable. It includes setting up policies and procedures to address the cloud service provider's cybersecurity setup, data privacy, and data recovery at termination.

5.4 Quick comparison between the methodology and current standards

Most standards address the specific issues of the ICT governance coverage and then recommend securing each section of the ICT installation (like securing a network or a web-service). The merits of these standards is that they provide the necessary guidelines in any implementation; however an implementation needs specific roles and responsibilities that are not considered in NIST and CIS, for example, but are required by ISO 27001 These standards imply the role and responsibility of organizations to implement the guidelines and recommendations as they see fit. The methodology covers these points and others, such as cyber-strategy, so that the standards can be fully implemented.

6 FINAL WORD IN 2021

The information in this paper will be relevant for only sometime (3–4 years); the methodology may be applicable for a longer "sometime" but eventually will become obsolete in 6–8 years. The standards are being regularly reviewed, and cybersecurity software are evolving. Nevertheless, the cybersecurity framework described in the methodology above will be applicable for some time. It could be augmented, developed, and amended until the introduction of new technologies related to ICT, which might have their own set of cybersecurity problems.

REFERENCES

[1] Meharchandani, D., 10 major cyber attacks witnessed globally in Q1 2021. https://securityboulevard.com/2021/04/10-major-cyber-attacks-witnessed-globally-in-q1-2021/.
[2] Selfkey, All data breaches in 2019–2021: An alarming timeline. https://selfkey.org/data-breaches-in-2019/.
[3] Winterburn, T., Pentagon blames 'Chinese hackers' for global Microsoft attacks. https://www.euroweeklynews.com/2021/03/06/pentagon-blames-chinese-hackers-for-global-microsoft-attacks/.
[4] Global HR, The role of hr in mitigating cyber security threats. https://www.ghrr.com/the-role-of-hr-in-mitigating-cyber-security-threats/.
[5] PA Knowledge, Putting human resources at the heart of cyber security. https://www.paconsulting.com/insights/putting-human-resources-at-the-heart-of-cyber-security/.
[6] Zielinski, D., Five top cybersecurity concerns for HR in 2019. https://www.shrm.org/resourcesandtools/hr-topics/technology/pages/top-cybersecurity-concerns-hr-2019.aspx.
[7] Williams, L., 22 BEST cyber security software tools in (2021 List). https://www.guru99.com/cybersecurity-software-tools.html.
[8] Cassetto, O., 21 top cyber security threats and how threat intelligence can help. https://www.exabeam.com/information-security/cyber-security-threat/.
[9] Centers for Disease Control and Prevention (CDC). Health Insurance Portability and Accountability Act of 1996 (HIPAA). https://www.cdc.gov/phlp/publications/topic/hipaa.html.
[10] PCI Security Standards Council, https://www.pcisecuritystandards.org/ and PCI Compliance Guide, https://www.pcicomplianceguide.org/faq/.
[11] The American Institute of CPAs (AICPA)'s, SOC 2® – SOC for Service Organizations: Trust Services Criteria. https://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/aicpasoc2report.html/.
[12] National Organization for Standards and Technology (NIST), NIST Cybersecurity Framework (CSF) Reference Tool. https://www.nist.gov/cyberframework/nist-cybersecurity-framework-csf-reference-tool.
[13] ISO, ISO/IEC 27001 Information Security Management. https://www.iso.org/isoiec-27001-information-security.html.
[14] Wikipedia, The CIS critical security controls for effective cyber defense. https://en.wikipedia.org/wiki/The_CIS_Critical_Security_Controls_for_Effective_Cyber_Defense.