Scientific Research Publishing

Journal of Information Security, 2023, 14, 212-226
https://www.scirp.org/journal/jis
ISSN Online: 2153-1242
ISSN Print: 2153-1234

Cybersecurity Requirements for Management Information Systems

Nadia K. Samara

Business Administration Department, Arab Open University, Amman, Jordan
Email: n_samara@aou.edu.jo

How to cite this paper: Samara, N.K. (2023) Cybersecurity Requirements for Management Information Systems. *Journal of Information Security*, **14**, 212-226.
https://doi.org/10.4236/jis.2023.143013

Received: March 25, 2023
Accepted: July 17, 2023
Published: July 20, 2023

Abstract

Cybersecurity is therefore one of the most important elements of security in developed countries. Especially since there is an overall trend towards cybersecurity in all aspects of life, I have found that the idea of cybersecurity is based on protecting critical facilities: The nation's information infrastructure. Information systems, including e-government management systems, are managed by key state agencies. As with economic, scientific, commercial, and other systems, threats are threats to a nation's national security. We have therefore found that many countries are preparing institutions capable of integrating cybersecurity into protection, development, and information security. This concept has become the most important concern of developed countries, which have secured all scientific possibilities and systems to achieve it. The electronic information network has become an integral part of today's daily lives in all places. In addition to personal uses, digital information is used, processed, stored, and shared. As this information increases and spreads, we have found that its protection has become more vital and has an effective impact on national security and technical progress.

Keywords

Cybersecurity, Security, Information Systems

1. Introduction

The issue of information security and protection is considered one of the most important issues of the era—the era of the fourth industrial revolution—where the success of any institution depends largely on the information it possesses [1]. But much information, systems, and infrastructure related to networks are exposed to danger from time to time [2]. As it is faced with various types of information breaches as well as exposure to criminal activities (hackers) that disrupt

its services and destroy its property. The hacker attacks vary from one side to another, from one place to another, and from time to time. This is done by using renewable, sophisticated hacking tools and mechanisms all the time. This confirms the importance of cybersecurity to maintain the security and safety of the homeland and its citizens [3].

The end of the Cold War led to the emergence of many challenges and threats that the international community had not witnessed before [4]. These challenges and threats are known as transnational threats because they do not recognize borders, national sovereignty, or the idea of the nation-state, which led to shifts in the security field and strategic studies as well as in the level of political practice [4].

In this context, many Arab countries sought to comprehensively develop their homelands, their security, their economy, the well-being of their citizens, and their decent living standards [5]. Renewable global, information technology (IT) systems and operational technology systems, prepare to deal with the data of artificial intelligence and the transformations of the fourth industrial revolution in line with the growth of computer processing capabilities and massive data storage and transmission capabilities [6].

This transformation requires the flow of information, its security, and the integration of its systems, as well as preserving and enhancing cybersecurity for Arab countries in order to protect the vital interests of countries, their national security, critical infrastructure, priority sectors, services, and government activities [7]. Therefore, a royal decree was issued to establish an organization named the National Authority for Cybersecurity in some countries, such as Saudi Arabia. This organization is the authority concerned with cybersecurity affairs and is considered the reference for the state for two purposes [8]. The first purpose is to protect its national security, its vital interests, and its sensitive infrastructure. The second purpose is to provide safe technical services and defense methods to protect data and communications systems from cyberattacks and to maintain the confidentiality and integrity of information [8].

- National Cyber Security Authority:

In addition to the emergence of threats and cybercrime, they pose a major challenge to national and international security, especially given the many implications arising from the evolution of the information revolution and the emergence of the digital age in the 21st century. Many researchers consider cyberspace to be the fifth arena of war after Earth, sea, air, and space [8].

This has created the need to ensure security in this digital environment. Cybersecurity has largely materialized with its emergence as a new dimension in the security research agenda that has attracted the attention of many researchers in this field. Cybersecurity research has become one of the latest innovations in the world's technological and digital development, and we can't afford to lose sight of it [9]. So, these technical studies in the field of digital computing have been a destination for many leading scientists around the world, but this digital development we are seeing has the potential to stabilize. There is another dark

aspect to attacks and hacks that can lead to this [10].

Hence the need to understand what cybersecurity is and to study it thoroughly in various respects as a new variable in international relations.

2. Search Problem

Despite the great positives achieved by IT, the escalating information revolution has come with many serious negative consequences as a result of its misuse. Among these new influences is the phenomenon of digital crime, whose dangers are escalating further and creating new types of crime like transcontinental crime. Its danger and dignity are no longer confined to certain countries and pose several legal challenges to crime prevention agencies.

Recently, the term "cybersecurity" has become popular, and many information security professionals have heard about what cybersecurity is, whether information security is part of cybersecurity, what the difference is between them, and many other questions that arise. Who does this term apply to, and what threats does cybersecurity protect against? Do they rest exclusively with institutions or with institutions and individuals, and how will they emerge from fourth-generation warfare to protect against.

Cyberspace has three dimensions. The first dimension is economic, which divides the Internet economy into two main areas: the first being the ICT industry, which includes hardware development, software production, and other services. The second is in the area of e-commerce by opening a free online marketplace. The second dimension is information security. Many countries allocate a significant portion of their budget to counter cyberattacks and update and develop their security systems. The third dimension is the security dimension, with the best example being the Cyber Threat Intelligence Integration Center (CTIIC) in the United States of America. This center coordinates among various other United States security agencies, such as the FBI, the CIA, and the National Security Agency.

In light of the above, the problem of research is identified in trying to answer the following question:

What are the requirements for achieving cybersecurity in management information systems in Arab countries seeking this?

3. Research Objective

The research aims to:

Know the requirements for achieving cybersecurity in management information systems in some Arab countries.

The importance of research:

The importance of research lies in the research itself, as educational studies in the field of cybersecurity are still limited, and terrorist attacks continue and may increase with technological development and the knowledge revolution. It also seems important to seek recommendations and proposals that support the cy-

bersecurity of Arab countries' management information systems.

Search Term:

Cybersecurity: "All procedures, measures, techniques, and tools used to protect the security of networks, software, and information from attack, loss, or illegal access and to secure devices and data."

4. Theoretical Framework and Previous Studies

Previous studies:

Arab Planning Institute (2019) Study on the Risks and Economic Implications of Cyberattacks: Case Study of the GCC Countries.

This study tried to highlight the importance of electronic risks and their economic impacts, how they are managed, and international models of incidents. Then, it resolved and assessed GCC situations as a model or case study, aimed at increasing interest in investing in cybersecurity and addressing gaps in economic planning to address these risks. Other GCC countries lead in some types of cyberattacks on economic activities, such as e-mail malware rates and spam ratios. The losses resulting from cyberattacks in GCC states also exceed the global average. Although GCC states' performance in countering cyberattacks has improved, the United Nations Global Cybersecurity Manual indicates that there are many legal, technical, organizational, training, and cooperative gaps that must be filled through improved performance, completion, and review of the current situation in these respects. Increased spending on its own is not enough to address threats and achieve cybersecurity in the GCC countries. Awareness, governance, and processes need to be improved because this region is one of the world's most advanced regions in the rapid adoption of modern technology.

Shetty Study (2019) on evaluating information security and privacy policies in educational institutions in Saudi Arabia, with application to the University of Qassim.

The study found the need for staff awareness programs, the promotion of cybersecurity research, and the importance of integrating and evaluating data in educational institutions.

Study (2020) El Hissi

The study attempted to propose a framework for cybersecurity governance in Morocco's public universities. It concluded that the use of cybersecurity in academic institutions would yield many administrative, material, and academic benefits.

Al-Otaibi Study (2017) on the Role of Cybersecurity in Enhancing Human Security:

The problem with the study was trying to answer a president's question: What is the role of cybersecurity in enhancing human security?

The study community is made up of cybersecurity workers at Saudi Aramco Branch Riyadh Region Sample Study (400 randomly selected individuals). The study used the analytical-descriptive curriculum.

One of the most important findings of the study is:

- ✓ Technical procedures for protecting the company's cyberspace are largely available, as the system is locked down if not used for a specified period of time.
- ✓ The company's cyberspace protection technical procedures are largely available, using biometrics (eye fingerprint, fingerprint, and sound fingerprint) for authorized passage.

The researcher recommended the need to pursue scientific and practical means of maintaining cybersecurity for governmental and private institutions and companies. He also recommended further study of the link between cybersecurity and human security.

Bakri Study (2017)

On information security in Sudanese university libraries. The aim of this was to identify the risks of not securing information and how to secure it for university libraries. The research used the historical curriculum by viewing published literature and the observation tool for Sudan's university libraries.

Study (Rehman 2016)

On the realities of cybersecurity management systems at higher education institutes in Pakistan's universities, it was recommended that there should be risk management in place and that security policies be developed to address these risks.

Previous studies in cybersecurity appear to be limited, but scientific research or theoretical literature also emphasized the need to study cybersecurity in multiple and changing forms. The current study is also moving in the same direction to promote the idea and culture of cybersecurity, especially in the university field, where it is almost entirely limited.

5. Cybersecurity

Cybersecurity Concept:

Meaning of cyber

Cyberspace is a relationship between the Internet and computers, and it means modern technology. It means all about computer networks, the Internet, and various applications like WhatsApp, Facebook, and hundreds of other applications.

Cybersecurity:

Cybersecurity aims to protect things through IT like hardware and software, which is called Information and Communication Technologies (ICT).

Cybersecurity means taking the necessary measures to protect cyberspace from cyberattacks through various technological means. The purpose is to systematically and administratively prevent unauthorized access, unlawful use, and systematic misuse of electronic information. This is done to maintain the continuity of available systems and information therein and protect privacy and confidentiality by following the necessary measures and procedures to protect data.

The Cybersecurity Terminology:

There are many concepts behind cybersecurity. It is defined as "a set of defensive decisions in the face of a cyberattack and its consequences, including the implementation of necessary countermeasures".

This is what Neittaanmaki Pekka and Leto Artti put out in their book Cybersecurity Analysis, Technology, and Automation, describing cybersecurity as "a defense against pirate attacks and their consequences, including the implementation of necessary countermeasures," which is defined as a series of actions to be taken.

Edward Amoroso identified Edward as a way to reduce the risk of attacks against software, computers, or networks, including tools used to combat piracy, detect and stop viruses, and provide encrypted communications.

In the ITU Communications Reform Directions Report 2010-2011, the Cybersecurity Community "uses a range of tasks such as compiling safety tools, policies, decisions, guidelines, crisis management methods, education, practice, best practices, and technologies that can be used to protect cyberspace environments, corporate assets, and users." The U.S. Department of Defense sets out a clear definition of the term cybersecurity. That is, "all regulatory decisions necessary for the protection of information in all its physical and electronic forms from various crimes and attacks on spyware".

The European declaration also showed that cybersecurity is the ability of information systems to resist attempts to penetrate their walls.

Note that cybersecurity is a deep concept of information security. Cybersecurity is concerned with the security of everything that is not on the Internet, and information security is not like this. It is related to the security of "paper" information, while cybersecurity is not like this [3].

Concepts associated with cybersecurity:

There are a lot of concepts related to cybersecurity, most notably:

Cyberspace: It was defined by the French Media Systems Security Agency (ANSSI) as "the communication space demonstrated through the global connectivity of digital information survey methods", a very sophisticated interactive environment, including physical and non-physical elements, consisting of a range of digital devices, networking systems, software, and users, which were important operators or users".

Cybersecurity Threats and it is affects:

There are many types of cybersecurity threats that countries around the world have faced and attacked their sectors, such as Phishing, Malware, Ransomware, Spyware, Trojans, Distributed Denial of Service (DDoS), Emotet, Man in the Middle, and SQL Injection.

Cybersecurity threats are becoming increasingly serious. Therefore, these threats could result in power outages, malfunctions with military hardware, and leaks of classified information. They may lead to the theft of priceless and private information, including medical records. They can disable systems, immobilize

phone and computer networks, and prevent access to data. It's not a stretch to imply that cyber dangers could have an impact on how life as we know it currently works.

To protect the personal data from these threats, there are many potential roles that are must take into accounts:

- ✓ Create a data backup.
- ✓ Keep software and hardware up to date.
- ✓ Pick strong passwords.
- ✓ Enable two-factor authentication.
- ✓ Use originality in your account recovery questions and responses.
- ✓ Steer clear of crucial transactions on public Wi-Fi.
- ✓ Be cautious about sharing personal information online.
- ✓ Set up an antivirus program and run routine virus checks.
- ✓ Use social media wisely.

Cybersecurity Awareness and Education:

Employee education and training in cybersecurity awareness is a continuous process that teaches employees about the dangers that lurk in cyberspace, how to stop them, and what to do in the event of a security crisis. Additionally, it fosters in them a sense of proactive accountability for safeguarding the company's assets. Cybersecurity awareness is simply being aware of security hazards and taking precautions to minimize risks.

Understanding cybersecurity includes being aware of the most recent security threats, cybersecurity best practices, the risks associated with using the internet, sharing sensitive information online, and other activities. Programs for raising security awareness increase your organization's security posture and tighten its processes, laying the groundwork for creating a more resilient company. For it to be most useful and effective, cybersecurity awareness must be a company-wide endeavor. The important of cybersecurity awareness and education are shown in the following points:

- Employees will be informed of information security best practices, apps, and technologies using a cybersecurity awareness program, including social media, email, and websites.
- How to prevent becoming a victim of these sneaky attacks.
- How hackers utilize malevolent methods.
- How they might be easy targets.
- It equips your personnel with the necessary information and tools to recognize and report any hazards before they cause any harm.
- Employees that receive cybersecurity awareness eduaction are better informed about common social engineering threats like phishing and spear phishing.

Cyber deterrence: Cyber deterrence is defined as preventing harmful actions against national assets in space and assets supporting space operations.

Cyberattack is defined as "undermining the functions and functions of the computer network for national or political purposes by exploiting specific weak-

nesses that allow the attacker to manipulate the system."

Cybercrime: Illicit acts and collections of acts carried out through machines, electronic devices, or the Internet.

Information Security:

This depends on three main themes represented by the CIA: confidentiality, integrity, and availability.

It's a technical group and an administrative procedure.

It also guarantees the full protection, confidentiality, and privacy of citizens' personal data. We will continue to work to protect computer equipment, information, and communications systems and services from change or damage.

Cybersecurity Objectives:

One of the most important objectives of cybersecurity:

- ✓ Strengthen technical operating system protection at all levels by hardening components such as hardware, software, services, and data.
- ✓ Response to attacks and information security incidents targeting government, public, and private sector organizations.
- ✓ Provide a reliable security environment for transactions in the information society.
- ✓ Critical infrastructure resilience to cyberattacks.
- ✓ Provide crisis requirements to reduce user-targeted risk and cybercrime.
- ✓ Eliminates weaknesses in many types of computer systems and mobile devices.
- ✓ Close gaps in your information security system.
- ✓ Resists malware intended to cause serious harm to users.
- ✓ Reduce spying and cybervandalism at the government and individual levels.
- ✓ Take all necessary measures to protect citizens and consumers alike from potential risks in different areas of Internet use.
- ✓ Training of individuals in new mechanisms and procedures to meet the challenges of hacking their technical devices with a view to damaging their personal information, whether by damage or with the intention of theft.

The importance of cybersecurity:

In today's networked world, everyone benefits from cyberdefense software. The importance of cybersecurity is as follows [4]:

- ✓ Preserving information and its integrity and homogeneity by stopping hands from messing with it, achieving abundance and readiness of data when needed.
- ✓ Protect devices and networks as a whole from hacks to be a protective shield for data and information.
- ✓ Explore and address weaknesses and gaps in systems.
- ✓ Use and develop open-source tools to achieve cybersecurity principles.
- ✓ Providing a very safe working environment while working on the web.

Importance of cybersecurity study:

There are a number of reasons why the study of cybersecurity is one of the most prominent areas in which the presence of qualified experts is needed to

protect the security of companies, institutions, and countries.

- ✓ The labour market is witnessing an ongoing need for cybersecurity experts.
- ✓ Working in cybersecurity can make a lot of financial sense.
- ✓ Cybersecurity expertise will be a goal for every distinct institution.
- ✓ Cybersecurity encompasses all practical areas, although they are different and diverse.
- ✓ Enabling the student to obtain unique privileges at work.

The most important career paths available after cybersecurity study:

This area is witnessing high demand and demand in various areas, so global reports and statistics indicate a significant increase in the demand for cybersecurity professionals. The cybersecurity market has grown significantly in all parts of the world. In 2004, it was estimated at $3.5 billion, while in 2015 it was costing $75 billion, and is expected to generate nearly $170 billion in 2020 [5].

Following a cybersecurity study and a bachelor's degree, the graduate will find many distinctive career opportunities in a number of areas. The career paths in this study vary, including:

Cloud Support Engineer, IT Support Specialist, Technical Support Engineer Software and Application Developer. Network Officer-Digital Forensic Officer.

Types of cybercrime:

Cybersecurity offenses include the following:

Infringement of information data, infringement of information systems, misuse of information devices or software offenses against funds, sexual exploitation of minors infringing on the intellectual property of digital businesses, Bank cards, and electronic money, crimes affecting personal information, racist crimes and crimes against humanity by informational means (cybercrime), crimes of gambling and the promotion of narcotics through online informatics, information crimes against the state and public safety, and offenses of encryption of information.

Causes of cybercrime [6]:

- ✓ In order to want to gather information and learn.
- ✓ Information and transaction management.
- ✓ Conquered the system and proved your superiority through the development of technological means.
- ✓ Harm to a person or entity.
- ✓ Achieve profit and material gain.
- ✓ Threats to national and military security.

Cybersecurity patterns:

The term applies to a variety of contexts, from business to mobile computing, and can be broadly divided into several general categories:

Network Security:

Around 1950, the first time this term was proposed, it is a way to protect computer networks from intrusive and opportunistic elements, whether they are targeted attackers or malware.

Application Security:

With a focus on protecting software and devices from threats, at-risk applications can provide access to data designed for protection. Successful implementation of the concept of security begins at the initial design stage, before any software or device is deployed.

Information Security:

Protect the integrity and privacy of your data, both at rest and during transportation.

Operational Security:

This includes processes and decisions to process and ensure the protection of data assets.

Cybersecurity Elements [7]:

In order to achieve the goal of cybersecurity, a set of elements must be available with each other to complement each other's roles, and the most important dimensions and elements of cybersecurity are:

- ✓ **(technology)**: Technology and technology play a critical role in individuals' and organizations' lives, providing them with superior protection against cyberattacks. This includes protecting devices in their various forms of smart, computing, and networking by relying on firewalls, using malware, antivirus, etc.
- ✓ **People**: Data and system users in an enterprise must use key data protection principles, such as powerful password identification and avoiding opening external links and attachments via e-mail, along with backups of data.
- ✓ **Process**: People and technologies are employed to carry out and conduct many operations and activities in line with applying cybersecurity foundations and responding efficiently to attacks.

Dimensions of Cybersecurity:

1) Military dimensions

The importance of cybersecurity in this dimension stems from the severity of cyberattacks and the breakthroughs that have led to wars and armed conflicts.

Breakthroughs in the system of nuclear installations and potential threats to national and governmental security that could result in disasters.

2) Political dimensions [8]

The political dimension of cybersecurity is based on the protection of national political systems and entities. There, technology can be used to transmit information and data, through which state and government security can be destabilized. Availability of published data and information.

3) Economic dimensions

Cybersecurity is highly concerned with preserving the economic interests of all countries. This is a close correlation between the economy and knowledge. Most countries are based on the production and distribution of knowledge and expertise at a level that enhances and develops their economies, demonstrating the clear role of cybersecurity in protecting their economies from theft.

4) Legal dimensions:

The multiple activities of individuals and companies are legally binding. With the emergence of the information society, new laws have been promulgated and a legal and regulatory environment has been regulated for the protection and preservation of rights in all parts of this society. This dimension of cybersecurity is based on the protection of the information society and helps to determine and enforce these laws.

Mechanisms (requirements) for achieving cybersecurity:

The simple steps below will help you maintain the right level of security and cybersecurity.

- ✓ **Reliability**: Using a reliable website is based on checking the URL when providing personal information, and if the site includes https at the beginning, it means that the site is safe. If you don't include http in the URL, it bypasses the need to enter sensitive information such as credit card data or social insurance numbers.
- ✓ **Fraudulent mail**: does not mean that email attachments are not attached or that you are not clicking on links to messages from unknown sources, as one of the most common ways in which people are stolen or hacked is through emails that are disguised as being sent from a trusted person.
- ✓ **Always-to-date**: there has been a constant concern for hardware development, most of which is software improvement, which contains correction of common errors to fix security problems. Successful hacker attacks are largely focused on older devices, which do not include sophisticated security software.
- ✓ **Backup**: This requires regular backups of files to prevent online security attacks.

Some of the requirements for achieving cybersecurity:

1) Leadership Commitment

Leadership commitment to be able to implement a successful cybersecurity plan, leadership needs to be on board due to the fact that cybersecurity affects all aspects of the organization and business. Without the leadership's involvement in the process, it will be complicated and even impede the development, implementation, and maintenance of safety protocols. The user will need the approval of senior management to enforce enterprise-wide security policies and guidelines. Once they adhere to the plan, the necessary resources and budget can be allocated to do the job.

2) Risk assessment

Risk assessment of the ability to identify cyberattacks: the user needs to assess risks at the beginning to identify and prioritize all threats; a risk assessment can be made by arranging the company's data and assets in order of priority based on the value that will be the last in case of theft or breach. For example, the list of leaked email IDs may be very harmful or may not be harmful. But stealing customer credit card records is not good, so you should prioritize anything that exceeds a certain threshold and is determined by total resources.

3) Data classification

Company-wide data classification is one of the initial steps to developing and implementing a cybersecurity plan, including a classification of what is private and what is general. For example, any information a user can publicly release will be all that their competitors can view without posing any risk to their company, such as advertising information or contact details.

On the other hand, private information such as new product development procedures and launch schedules should only be accessed by employees or partners on the basis of the need for knowledge. The additional classification of data may include who has access to any kind of data and to what extent, how data should be stored or shared, how it is backed up, etc.

4) Cyber flexibility

Cyber flexibility and business continuity planning Once you take the right security measures, the enterprise will feel confident in its ability to defend against any attack that may come its way; however, the user should also consider the possibility of failing or getting things out of control altogether. In such cases, it needs to have a recovery mechanism.

6. So, Application Requirements

Many financial and commercial institutions are establishing specialized organizational units for information management and security, either through one organizational unit for information management and protection or two separate information management units, one for information security management. The Information Management Unit (IMU) includes processes for data sources, information, and processes and their relationship to objectives. The Information Security Management Unit includes information protection operations, surveillance and protection of computer equipment, and response to security events. This unit contains a special center called the Cyber Security Operation Center [10].

In order to implement this framework, each institution will need to identify those responsible for conducting these processes and events. Since the COBIT 5 scale is primarily concerned with these operations and events, the RACI Responsibility Allocation Table is guided by this scale of these processes and activities within various organizational units. This is so that the disciplines necessary for cybersecurity can guide NIST's Cybersecurity Job Distribution Table.

To improve institutions' information security governance, the following needs to be done:

1) Developing effective information management in each organization through a new organizational unit to:

- ✓ Build and manage the structure of the chains of objectives from institutional objectives to organizational units.
- ✓ Build and manage the structure of operations in these institutions, their relationships with each other, and their relationship with the structure of objec-

tives.

- ✓ Building and managing the structure of the enterprise's data and information, its relationships with each other, and its places of creation, use, transfer, storage, and destruction.

2) Developing information security management by focusing work in a new central unit to:

- ✓ Build and manage the structure of access and data handling powers according to information classification tables.
- ✓ Build and manage the structure and powers of data users.
- ✓ Follow-up on the implementation and modification of policies related to the security and protection of information, such as the security and protection of information policy and its associated policies, with the relevant authorities.
- ✓ Study and assess information security risks with relevant entities.
- ✓ Ensure that the institution's operations comply with international and domestic laws and legislation in relation to the handling of information.
- ✓ Follow-up on the requirements of the boards of directors regarding their requirements for the security and protection of information in the enterprise and develop and update a security and information protection strategy and policy accordingly.

3) Develop cybersecurity management effectiveness through a separate organizational unit to:

- ✓ Perform the necessary technical procedures to protect computer infrastructure in accordance with security requirements and policies.
- ✓ Continuous monitoring and monitoring of computer infrastructure security through the Security Operation Center.
- ✓ Ensure the effectiveness of systems and procedures for detecting security events in computer infrastructure.
- ✓ Respond to security events and implement the necessary procedures to deal with them and minimize their impact within business continuity plans.
- ✓ Work with all relevant authorities to restore the computer infrastructure as usual.

7. Conclusion

Cybersecurity is therefore one of the most important elements of security in developed countries. Especially since there is an overall trend towards cybersecurity in all aspects of life, I have found that the idea of cybersecurity is based on protecting critical facilities, such as the nation's information infrastructure. Information systems, including e-government management systems, are managed by key state agencies. As with economic, scientific, commercial, and other systems, threats are threats to a nation's national security. We have therefore found that many countries are preparing institutions capable of integrating cybersecurity into protection, development, and information security. This concept has become the most important concern of developed countries, which have secured

all scientific possibilities and systems to achieve it.

The electronic information network has become an integral part of today's daily lives in all places. In addition to personal uses, digital information is used, processed, stored, and shared. As this information increases and spreads, we have found that its protection has become more vital and has an effective impact on national security and technical progress.

Accordingly, We Recommend

- Emphasize the need to take care of the requirements of protecting administrative information systems.
- Incorporate cyberspace into the curriculum of education.
- Promote cybersecurity research and studies in master's and doctoral theses.
- Promote areas of scientific research and innovation in the field of cybersecurity.
- Raising workers' awareness of all state institutions and developing professional standards and establishing infrastructure to enter the global software industry and the ability to compete with the imported product.
- Encourage civil society organizations and emphasize their active role in dealing with the unsafe use of information technology through scientific activities and the dissemination of a culture of security use of the Internet and modern digital applications.
- Encouraging investment in cybersecurity. The investment is divided into two sides. The first is the localization of cybersecurity technology and infrastructure. The second is the development of skills and expertise to possess national capabilities capable of building, managing, analysing and developing cybersecurity systems.
- Further scientific studies on the issue of information security.
- Ongoing training courses for information workers.

Conflicts of Interest

The author declares no conflicts of interest regarding the publication of this paper.

References

[1] El Hissi, Y. and Arezki, S. (2018) Conceptualization of an Information System Governance Model Dedicated to the Governance of Scientific Research in Moroccan University. 2018 4*th International Conference on Computer and Technology Applications* (*ICCTA*), Istanbul, 3-5 May 2018, 54-58. https://doi.org/10.1109/CATA.2018.8398655

[2] Rehman, H., Masood, A. and Cheema, A. (2013) Information Security Management in Academic Institutes of Pakistan. 2*nd National Conference of Information Assurance* (*NCIA*), Rawalpindi, 11-12 December 2013, 47-51. https://doi.org/10.1109/NCIA.2013.6725323

[3] Anton, I. and Mamedov, O. (2017) The Return of Mamba Ransomware Secure

List-Information about Viruses, Hackers and Spam.

[4] Brotby, K. (2009) Information Security Governance: A Practical Development and Implementation Approach (Vol. 53).

[5] Security for Industrial Automation and Control Systems: Establishing an Industrial 900 Automation and Control Systems Security Program.

[6] Force, J.T. and Initiative, T. (2013) Security and Privacy Controls for Federal Information Systems and Organizations. *NIST Special Publication*, **800**, 8-13.

[7] Center for Internet Security (CIS) Critical Security Controls for Effective Cyber Defense (CSC). https://www.cisecurity.org 899.

[8] National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity V1.1.

[9] Draft NIST Special Publication 800-181 NICE Cybersecurity Workforce Framework (NCWF) National Initiative for Cybersecurity Education (NICE).

[10] Control Objectives for Information and Related Technology (COBIT). https://www.isaca.org/resources/cobit