Naif Arab University for Security Sciences
Journal of Information Security & Cybercrimes Research
مجلة بحوث أمن المعلومات والجرائم السيبرانية
https://journals.nauss.edu.sa/index.php/JISCR
JISCR

The Role of Governance in Achieving Sustainable Cybersecurity for Business Corporations

Shahad A. Alashi*, Dhuha H. Badi
Department of Information Science, King Abdulaziz University, Jeddah, Saudi Arabia.

Received 15 Jul. 2020; Accepted 12 Oct. 2020; Available Online 15 Dec. 2020

Abstract

The study discusses the role of governance in the sustainability of cybersecurity for business corporations. Its objectives focus on tracking technology developments and their impact on industrial espionage attacks and theft of industrial intellectual property. It also identifies the indicators and effects of such espionage and theft on business corporations. The study is based on the content analysis methodology for analyzing intellectual production pertinent to cybersecurity governance and industrial cyber espionage. The study concludes that relying on information and communication technology without adopting a cybersecurity integrated approach including technical, organizational, and social measures leads to the disclosure of a corporation's trade secrets by unauthorized persons. Moreover, loss of competitive advantage and damage to the corporate's financial affairs and reputation may occur. The most important indicators of the study predicting dangers affecting business corporations are the absence of a strategic plan for cybersecurity, inefficient programs for training and cybersecurity awareness, and a lack of secure infrastructure. The vulnerability of business corporations to breaches has many implications. The study shows that cybersecurity governance in turn prepares the corporation to encounter risks targeting its trade secrets. The study finds that there are three integrated elements processes, technology, and persons, for establishing an effective cybersecurity governance program. Accordingly, the main aspects of cybersecurity governance can be employed. The study highlights a range of challenges that business corporations may face when implementing the cybersecurity governance program. These challenges are related to cybersecurity strategy, unified processes, implementation and accountability, senior leadership control, and resources.

I. Introduction

The security of infrastructure and cyber systems has become more necessary than ever. This great necessity arises from the intensive digitalization of all activities in life. Therefore, prevention of cybercrimes, cyberwars, online fraud, and cyber theft is a critical requirement for all individuals, communities, corporations, and governments. Cybercrimes are increasing; they threaten personal privacy, work methods, and processes. This threat extends to affect industrial intellectual property and government sovereignty [1]. Business corporations are more vulnerable to cybercrimes. Sensitive information about such corporations is vulnerable to unprecedented risks. When such information is stored on networks, they will be considerably subject to cyberattacks. In most cases, measures and procedures ensuring sensitive information protection are not taken or implemented because of high cost or misunderstanding of the problem. Accordingly,

Keywords: *Cybersecurity, Industrial Cyber Espionage, Theft of Trade Secrets, Cybersecurity Governance, Business Security.*

Production and hosting by NAUSS

* Corresponding Author: Shahad A. Alashi
Email: Alashi@gmail.com
doi: 10.26735/EINT7997

business corporations looking forward to competition and success must take all necessary precautions to protect their sensitive assets. Otherwise, such corporations will be threatened by industrial cyber espionage committed for commercial purposes, not for security or national ones. This type of espionage may be committed by governments or other competitive corporations trying to get information related to other corporations to gain industrial or commercial benefits. The targets of industrial cyber espionage include corporation development research, designs, formulas, industry processes, and future plans [2].

Business corporations are facing cybersecurity challenges that are highly associated with the theft of trade secrets and industrial intellectual property through cyber hacking attacks. Therefore, the governance concept application is necessary for a positive contribution to fighting cyberattacks. Subsequently, the security of trade secrets can be achieved, and sustainable cybersecurity may be actualized. Sustainable cybersecurity is related to "provision of sustainable security practices, such as confidentiality and safety, for information and institutional assets that are necessary to achieve sustainable development. Moreover, sustainable cybersecurity should have an extensive vision to treat both current and future issues and protect the market position and strategic rank of business corporations." [3]. The concept of governance can be defined in the context of cybersecurity as a subgroup of corporations' governance focusing on clear administrative principles, bases, policies, procedures, and rules characterized by validity and transparency to recognize and manage cyber risks. Accordingly, a framework for corporations' activities can be set up for transition to cybersecurity [4]. Such principles and policies can also offer strategic guidance for security activities and ensure achievement of cybersecurity objectives, such as risk confrontation and resource management. The corporations' boards of directors should develop and maintain a framework supporting cybersecurity and aligning with corporate objectives [5]. They identify how business corporations can discover and combat industrial cyber espionage. The application of the cybersecurity concept is very important. This study seeks to identify the role of governance in achieving sustainable cybersecurity for business corporations. There are many relevant aspects such as the impacts of technological developments on industrial espionage attacks and theft of industrial intellectual property, as well as the indicators of industrial cyber espionage and theft of industrial intellectual property and their repercussions on business corporations. Another aspect includes the effect of governance on cybersecurity sustainability in light of the development of industrial espionage attacks and theft of industrial intellectual property.

The increasing development of information and communication technology has motivated economic aspects of growth in business corporations, which represents the study problem. It offers many advantages that include storing of and access to confidential information. On the other hand, this development has created an environment that threatens industrial intellectual property and trade secrets. This may encourage competitive corporations and governments to target trade secrets and cause physical damage. In general, this new environment can exploit the weak points of information and communication technology operating hundreds or thousands of laptops, servers, tablets, smart phones, and relevant software linked together to achieve private objectives. There is a lot of news on violations affecting corporations and cyber wars leading to the breakdown of industries. Therefore, there is a need for investment in cybersecurity to protect assets and trade secrets constituting a competitive advantage by employing components of cybersecurity governance. Accordingly, we can identify the study problem in the following question: What is the role of governance in achieving sustainable cybersecurity for business corporations?

Industrial cyber espionage and theft of trade secrets leading to violation of the industrial intellectual property of companies are important to this study. As a result of these crimes, corporations may collapse or suffer bankruptcy. The study importance arises from the importance of the study topic that seeks to discuss how the economies of business corporations and countries are negatively affected. The study highlights the role of governance in sustaining cybersecurity to protect trade secrets and industrial intellectual property. We can realize the importance of this study through the demonstration of the positive impact resulting from application of components and concepts of cybersecurity governance on business corporations to achieve sustainable cybersecurity. To the best of the researchers' knowledge, studies examining the role of governance in achieving sustainable cybersecurity in business corporations are rare. Therefore, the study enriches the research literature associated with the study field.

In general, the study seeks to highlight the importance of applying cybersecurity governance components

to business corporations and explores the scientific contributions of specialized intellectual production. The study's main objective is to look into technological advancements and their impacts on industrial espionage attacks and theft of industrial intellectual property. In addition, other important aims include the identification of indicators and impacts of industrial cyber espionage and theft of industrial intellectual property on business corporations and the role of governance in achieving sustainable cybersecurity to combat the development of industrial espionage attacks and theft of industrial intellectual property.

The study attempts, through the problem statement, to answer the following questions: How has technological progress changed methods of attack associated with industrial espionage and theft of industrial intellectual property? What are the indicators and impacts resulting from industrial cyber espionage and theft of industrial intellectual property of business corporations? How can business corporations employ governance to achieve sustainable cybersecurity?

To achieve the study objectives, the content analysis methodology is employed to analyze studies and intellectual production associated with industrial cyber espionage, the theft of trade secrets, and cybersecurity governance. Accordingly, the relationship between governance and sustainable cybersecurity can be explored. This methodology also assists in developing a common vision to indicate how business corporations can benefit from cybersecurity governance to achieve sustainable cybersecurity that ensures protection of trade secrets and industrial intellectual property.

II. Literature Review

The previous studies constituted an important base when preparing this study. By reviewing the literature, the researchers try to explore the positive impact of governance on cybersecurity sustainability for business corporations. Moreover, the researchers examine the repercussions of industrial espionage attacks on cybersecurity. They discover the role of governance in achieving cybersecurity for business corporations. In this section, the literature is reviewed and chronologically arranged from the newest to the oldest (from 2020 to 2016). The topic of cybersecurity is developing, so it is important to rely on the most recent studies. These studies are as follows:

Konopatsch [6]: The study highlights the crimes of economic and industrial espionage. It analyzes the structure, framework, and legal concepts of economic and industrial espionage in Austria and Switzerland. When comparing between legal systems applied in Austria and Switzerland, the study shows many similarities and basic differences. It also indicates that no new amendments concerning crimes of economic and industrial espionage are made for both legal systems. Therefore, crimes are increasing because the legal structures of both systems are based on inaccurate drafting that can provide law enforcement authorities with different interpretations. The study demonstrates that neither legislatures in Austria and Switzerland nor law enforcement authorities have employed all criminal law capabilities for fighting industrial and economic espionage. It suggests that drafting of laws should be given more attention, to enable law enforcement authorities to efficiently combat economic and industrial espionage [6].

Sadok el at. [7]: The study indicates that industrial cyber espionage results from misunderstanding of security controls, weak connectivity inside organizations, and a lack of shared values between employer and employee. These vulnerabilities create gaps that may be easily exploited. Therefore, the study seeks to define the social and technical approaches that may be employed to counter industrial cyber espionage. The security failures contributing to internal threats are also demonstrated. The study shows that work systems interdependence on both human and artificial intelligence and rapid technological changes make it difficult for designers to understand and predict all vulnerabilities and threats. It highlights that employees constitute the most vulnerable component regarding security procedures.

Vasiu [8]: The study analyzes a large corpus of data including cases brought to courts, cybersecurity reports, and press releases examining the main cybersecurity risks grouped into three broad categories: damage, theft of trade secrets, and payment fraud. It stresses that strategies, policies, and programs of cybersecurity should be improved, and actions taken for controlling risks threatening cybersecurity should not be restricted to only technical procedures, but they should also include legal and regulatory measures. Vinnakota [9] explores the governance aspects of cybersecurity in enterprises. The study suggests a cybernetic model for continuous and good governance of cybersecurity leveraging multidisciplinary collaboration, goal directedness, and dynamic control aspects of cybernetics. The implementation of the cybernetic model in a big telecom enterprise improved its systems and processes of cybersecurity governance. The

enterprise board of directors became aware of increasing risks arising from cyberattacks and performed more supervisory duties to ensure cybersecurity risk management. De Brauin & von Solms [10] discuss adaptations to a cybersecurity governance maturity model. Their study indicates how this model can be used for organizational aspects to create descriptive and understandable reports for the various roles within the board of directors and executive management. The study also sheds light on cybersecurity and cybersecurity governance and demonstrates how cybersecurity governance is associated with information security. It describes the risks and threats affecting cybersecurity and how some of them are developing. The study suggests some steps that must be taken when using the cybersecurity governance model. These steps include model scope evaluation, using the model as part of an audit session, evaluation of models, creation of reports, submission of reports and reassessment of maturity.

It is important to note that the previous studies indicate that clear laws including detailed articles should be enacted to protect the afflicted parties in cases of industrial and economic cyber espionage. Moreover, organizational and social aspects should be addressed, and technical measures should be taken. Industrial cyber espionage results from increasing reliance on technology. Therefore, some studies suggest models for continuous and good governance of cybersecurity. Such models can ensure cybersecurity sustainability in corporations to control and manage cyber risks. This allows anticipatory prediction of cyberattacks and cyber risks. The previous studies also demonstrate steps for using models of cybersecurity governance. They show that strategies, policies, and programs should be prepared to ensure effective cybersecurity. Our study includes two parts: the first part is associated with cybersecurity governance, while the second one demonstrates the study's intellectual framework.

III. Related Works and Literature Review

This part offers some conceptual and theoretical bases to understand industrial espionage and the impacts of technological developments. It provides a mechanism for countering industrial espionage in business corporations, based upon reviewing the abovementioned literature. We believe that cybersecurity governance should pay attention to various processes, techniques, and persons and to their relevant elements. We argue that selection of governance structure should include dimensions and components to achieve sustainable cybersecurity. Lastly, this part highlights challenges that may impede the application of cybersecurity governance in business corporations.

A. What is the Definition of Industrial Espionage?

Industrial espionage is defined as theft of a corporation's secret and sensitive trade information to be utilized by its competitors [11]. Industrial espionage may be organized by foreign intelligence bodies (government espionage) or by competitive corporations (industrial espionage) at the hands of human experts [12]. Button [13] defines economic espionage as targeting or acquiring trade secrets from domestic companies or government entities for the benefit of a foreign state. This indicates that industrial espionage is the same as economic espionage, except that rather than benefitting a foreign government, it benefits another private entity. Spies focus on trade secrets associated with investments represented by redevelopment, innovation, and invention. These aspects are often basic factors for developing and maintaining competitive advantages. Trade secrets generally include technical data and secret work data including customer contact information, pricing information, and purchasing records [8].

Industrial espionage may take many forms, such as theft of technical specifications and formulas, processes, designs, and equipment for sophisticated electronic surveillance. It also includes employee bribery or extortion. Theft of trade secrets or espionage related to work activities may be dated to the early period of performing trade and commerce processes by people [11].

The researchers give a procedural definition for industrial cyber espionage as the hacking of cyber systems of business corporations by foreign parties for accessing competitive secret information that is valuable for this business corporation. This secret information may uncover competitors' activities related to new products, special assemblies, important research fields, and production approach and quantity. Industrial cyber espionage is committed to control markets, gain profits, and acquire research or studies.

B. Technology Advancements and their Impacts on Industrial Espionage Attacks and Intellectual Property Theft

The methods employed for committing industrial espionage and theft of trade secrets have developed. They

have changed over the years. Before the age of digitalization, such methods were based on direct access to information. Therefore, secret information was kept in places that were difficult to access to prevent theft and track theft crimes. During the age of digitalization, most information or data are saved on computers, servers, or networks [14]. In the past, business corporations seeking to steal a competitor's trade secrets had to bribe such competitors' employees. Now, industrial espionage and trade secret theft have become easier [15]. The digital transformation of information everywhere, broad connectivity of work systems, and techniques of the fourth industrial revolution, including artificial intelligence [1] and the internet of things, facilitate industrial espionage through the internet. Most incidents of industrial cyber espionage result from the weak security structure of corporations. Moreover, internal threats constitute an important pattern for industrial cyber espionage [7]. Spies try to access sensitive information associated with trade secrets of a corporation's economy. More dependence on information and communication technology creates concerns regarding security, because weak and unprotected systems constitute a gap enabling hackers to access information and trade secrets.

C. Indicators of Industrial Cyber Espionage and Theft of Industrial Intellectual Property for Business Corporations

Industrial espionage has increased all over the world, particularly during recent years. It has escalating dangers and negative effects. It affects not only persons, but also national and world economies in general. The Accenture Security & Ponemon Institute conducted a study on the increasing participation of governmental actors in targeting non-military data. This study includes 355 companies across 11 countries in 16 industries. It shows that there is an increasing level of economic espionage including theft of high-value intellectual property by nation-states [16]. Clement [17] presents statistics from 2019 for the global sectors that were most targeted by cyber espionage, showing that the manufacturing sector was ranked first with 75 cyber espionage incidents, as shown in Fig. 1.

Before the occurrence of industrial cyber espionage and violations of industrial intellectual property, the researchers conclude that there are many indicators constituting an alert to expected dangers. Business corporations should pay attention to such dangers that may be represented by the absence of:

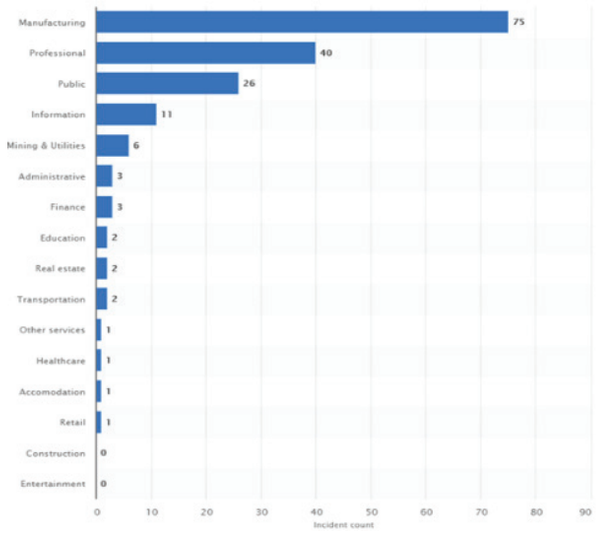

Fig. 1. Global industry sectors most targeted by cyber espionage

1. A strategic cybersecurity plan
2. Effective training and awareness programs provided for employees
3. A plan including policies, processes, procedures, and best practices for reducing cyberthreats
4. Developed programs for managing cyber risks
5. Continuous evaluation and management for risks threatening companies
6. Risks recovery plans
7. A developed private infrastructure for information technology and security

We see that the absence of cybersecurity governance elements paves the way for industrial cyber espionage threatening business corporations.

D. Impacts of Industrial Cyber Espionage and intellectual Property Theft on Business Corporations

Cyberattacks constitute the most critical challenges for businesses. They have many repercussions on business corporations. Khari et al. [18] show these repercussions as follows:

1. Loss of earnings
2. Defamation of the corporation
3. Data normalization or loss
4. Interruption of business processes
5. Undermining trust of corporation customers

6. Undermining investors' trust
7. Legal consequences

Rothke [19] adds two important repercussions: loss of market share and low commercial budget.

E. Models for Industrial Cyber Espionage and Targeting of Corporations' Trade Secrets

Large investments made by business corporations for developing industrial intellectual property are profitable for any party desiring to invest in such businesses. Therefore, theft of trade secrets spreads through cyberattacks. Although such theft targets big companies or government bodies, it affects all companies, regardless of their size or sectors. There are many forms of cyberattacks that seek to spy on work secrets. The espionage is committed by placing malicious software into databases, applications, and systems. It is also carried out by spying on and reading data submitted over networks. Attackers can spy on companies work secrets by using different methods not noticed by such companies. In this part, we present some models of industrial cyber espionage that target some corporations as follows:

- The wiper attack made by Iran against Saudi Aramco in 2012. This attack was dangerous, as it wiped all Aramco's computers and resulted in tremendous damages for Aramco and for the Kingdom of Saudi Arabia. The financial losses related to costs of work and computers that had to be replaced reached tens of millions of dollars at least [20].
- The Italian oil services company Saipem was attacked by hackers in December 2018. These hackers used the Shamoon variant virus. They crippled hundreds of the company's servers and computers [21].
- In March 2019, Iranian hackers targeted thousands of people working at more than 200 oil, gas, and heavy machinery companies around the world [21].

This type of cyberattack seeks to steal oil companies' secrets and wipe data from computers. It may also try to overcome competitors.

- Hackers sponsored by China were identified in August 2019. They had committed cyber espionage against many cancer institutes in the USA [21].
- In the international competition by researchers, companies, and governments to find a COVID-19 vaccine, agencies combating espionage in each country are seeking protection of their efforts. However, such efforts are targeted by foreign agencies. The USA has monitored attempts by foreign agencies of cyber espionage to explore research on COVID-19 vaccine production. Security bodies in Britain have indicated that they have noticed similar activities. They also show that there are many expectations that foreign intelligence bodies, including the Chinese Communist Party, will try to obtain research findings [22].

It is worth mentioning that companies are looking to obtain research to fabricate medications and vaccines for commercial benefit.

- The Norwegian company Visma declared in February 2019 that it was attacked by hackers belonging to the Chinese Ministry of State Security. Such hackers tried to steal trade secrets from the company's clients [21].
- Westinghouse company, the manufacturer of the most famous and strongest nuclear reactor, declared its bankruptcy in 2017. The company's computers were hacked and the reactor design stolen. A Chinese company manufactured the reactor without bearing the research and development cost [23].
- Trade secrets information was stolen from the SolarWorld company. Subsequently, it declared its bankruptcy in 2017 [23].
- One of the most dangerous cyberattacks were made by Chinese hackers against two of the largest companies for steel manufacturing, Alcoa and ATI, in 2008. Such hackers installed malicious software on the computers of the two companies producing aluminum used for manufacturing spacecrafts, planes, military vehicles, cars, electronics, oil and gas digging equipment, building materials, and manufacturing equipment. The hackers' goal was to steal the two companies' trade secrets that are required for the Chinese companies to manufacture high-quality stainless steel. The same group of hackers have used malicious software to steal trade secrets related to the solar cells factory at SolarWorld, Allegheny Technologies Inc, and United Steel Works. The

SolarWorld company indicated that the solar cells mechanism was stolen to be developed and sold to a Chinese competitor [23].

Some models on industrial cyber espionage around the world have been demonstrated. Many cases of industrial cyber espionage have been published or declared by companies. However, other companies refused to declare cyber espionage cases as they were afraid that such cases would negatively affect their reputation or market rank. The formal director of the FBI Robert Mueller expounded that there are two types of companies: companies hacked and companies that will be hacked [25]. Therefore, the cyber threat is multi-faced and incremental. It has a negative effect on the final productivity of business corporations. The abovementioned models indicated that companies have not implemented the necessary procedures to protect their trade secrets and strengthen their cybersecurity. These procedures include technical, organizational, or social measures that are covered by the term governance. There is no doubt that cybersecurity represents a main advantage for companies in general, and particularly for business corporations. It also constitutes a fundamental factor for sustainable economic development. Therefore, ways for achieving sustainable cybersecurity for business corporations should be identified to maintain industrial intellectual property and trade secrets.

IV. The Role of Governance in Sustaining Cybersecurity for Business Corporations in the Light of Development of Industrial Cyber Espionage and Theft of Intellectual Property

Cybersecurity has become a necessary requirement. Cybercrimes have become not only a technical problem, but they also create a commercial problem [26]. They threaten business corporations. Therefore, regulatory leaders of business corporations should work to lay down suitable governance frameworks for regulating and controlling a corporation's cybersecurity and cyberspace.

Governance plays a very important role in achieving the security objective of business corporations. It does not satisfy the current requirements only, but also ensures effective plans for dealing with future challenges. We need a cultural transition enabling corporations to overcome cybersecurity threats constituting a commercial problem and pay attention to financial risks. The participation of corporations' leaders is very important. The leaders have knowledge and a vision for identifying corporations' budgets and priorities and how corporations can overcome risks. This is the leadership-based approach [27].

Bubaker & Nguyen [28] believe that the necessity of business corporation governance is driven by many factors that include the following:

- Contribution to maintenance or increasing of shareholders' value
- Regaining trust in stock markets
- Potential of corporations' long-term success and sustainability of profits
- Corporations adopting good practices of governance and following good policies and practices for social responsibility are likely to be more sustainable in the long term.

Therefore, we can say that achieving cybersecurity governance at the business corporations level leads to sustainable cybersecurity. As mentioned in the study introduction, cybersecurity governance is part of corporation governance. The researchers indicate that cybersecurity governance is an integral part of corporation governance because of the large transition to cyber space. The business corporations that adopt cybersecurity governance, follow clear, sound, and transparent principles, policies, laws, and procedures, and implement awareness and training programs for employees are more sustainable in the long term. Theft of trade secrets exhausts corporations. To prevent or reduce such a type of theft, corporations must evaluate the risks, costs, and benefits of cybersecurity and trade secrecy by investing in cybersecurity governance. Cybersecurity governance for business corporations can be procedurally defined as the corporation's strategy for administering the security of trade secrets; maintaining industrial intellectual property through adoption of bases, rules, security policies, and procedures; applying technical controls and managing risks; and increasing awareness of employees.

For future challenges, the governance framework should continually focus on the threats that are arising and the rapid changes affecting the technology environment. However, changes driven by a system of quality assurance management that is made for work culture represents a more important factor [26]. Accordingly, trade secrets and threats can be maintained and avoided. Cybersecurity technology is not enough to protect business corporations. Therefore, it should be incorporated with a supportive regulatory framework that can maintain sensitive digital assets of business corporations.

A. The Targets of Cybersecurity Governance for Business Corporations

By applying its elements, cybersecurity governance is seeking to achieve many objectives for business corporations. Hawes [29] proposes a number of objectives:

- Classification and mitigation of risks and threats affecting trade secrets and industrial intellectual property
- Corporations' preparedness to be aware of cybercrimes and security breaches associated with trade secrets. Subsequently, such threats can be confronted, and recovery may be achieved.
- Offering a way for executive management to understand risk levels and set precautions for encountering industrial cyber espionage
- Identifying an approach based on expected risks that may affect persons, systems and technology that are used daily
- In [30], authors add that roles, responsibilities, and security accountability should be identified to reduce overlapping of procedures. This can be employed for measuring performance and progress
- The researchers who prepared this study indicate that cybersecurity governance seeks to achieve sustainable cybersecurity for business corporations. Cybersecurity should balance between providing business corporations with security needs and identifying the cost required for maintaining this security.

Cybersecurity governance for business corporations is important. It focuses on trade secrets protection and assists in the transition from a reactive approach to a proactive approach to monitor potential threats and risks arising from industrial cyber espionage [29]. Passman [31] summarizes that the importance of cybersecurity, if it is implemented in a good manner, is represented by offering necessary technology, persons, processes, and legal procedures to protect corporations' trade secrets and other secret data. This is a critical factor to achieve cybersecurity governance.

B. Cybersecurity Governance for Business Corporations

Researchers propose that cybersecurity includes a comprehensive package of security practices. These practices cover information security, information technology security, and other relevant practices [32]. Cybersecurity consists of various factors interfering and integrating with each other to achieve the required security goal for corporations. To achieve effective governance of cybersecurity for corporations, it is essential to integrate three main elements: processes, technology, and persons. Accordingly, a coherent approach leading to sustainable cybersecurity can be identified [33]. For accurate demonstration and identification, we indicate how these three elements can be integrated with basic dimensions of cybersecurity governance for achieving sustainable cybersecurity for business corporations.

1) Processes:

Processes represent the regulatory measures identifying and demonstrating how to employ many regulatory activities, procedures, roles, and documents for mitigating risks threatening a corporation's information. These measures represent the key for implementing an effective strategy for cybersecurity. Standards of ISO "ISO 27001" related to cybersecurity processes can constitute a base for identifying continuous evaluation and improvement and implementing a security management system. Moreover, the regulatory measures can present some ready tools for authentication to lay down policies, procedures, work instructions, and roles. They provide us with the necessary requirements to apply standards with no associated complications or costs [33].

There are many themes associated with the processes element. These themes should be given attention when implementing cybersecurity governance. They include the following:

- **Cybersecurity Strategy [34]:** For developing an effective strategy for cybersecurity, the cybersecurity risks should be associated with work processes, and strategic objectives for corporations should be identified. In addition, setting scope, cybersecurity needs, and key performance indicators (KPIs) is a necessary requirement to implement a cybersecurity strategy. This strategy is associated with resource needs and continuous monitoring processes. There are many plans that should be incorporated within a cybersecurity strategy. These plans include proactive plans for managing risks that are considered a critical factor for any successful strategic plan. The proactive plans include predictions for risks and design solutions, instead of taking reactive actions after

damage occurrence. They adopt the proactive approach to identify, predict, analyze, control, or eliminate risks before causing damage to work, budgets, or net profits [36]. Moreover, the proactive plans include measures for recovery and continuity to be ready to deal with sudden events. An example of proactive measures can be represented by keeping a backup copy of important data by the corporation in a remote location. This backup copy can contribute to rapid recovery from incidents [18].

- **Cybersecurity Management [34]:** To effectively create programs for cybersecurity management, the following principles should be observed:
  - Setting policies and objectives for information security. These policies and objectives should be compatible to the corporation's strategic attitude.
  - The system requirements for managing information security should be integrated with the corporation's processes.
  - The resources necessary for the system of information security management should be available.
  - The system requirements for managing information security should be observed.
  - The system of information security management should achieve the desired outcomes.
  - Guiding and supporting employees to contribute to the efficacy of the system of information security management.
  - The improvements should be continually promoted [35].
- **Policies and Procedures of Cybersecurity [34]:** The security policy constitutes some rules and processes issued by the corporation's senior leadership. It describes controls and security activities for the corporation and shows a mechanism for protecting important digital assets. Supportive procedures should be taken to implement the security policy aspects related to the protection of trade secrets that must be obligatory for employees and third parties [37]. The security policy does not identify a technical solution, but it focuses on conditions assisting in asset protection. However, it is efficient in organizing business and directing users. The security policy should be written and declared. It also should cover the physical security, employee's affairs administration, devices, and software [38]. The business corporation should develop a comprehensive set of policies to protect trade secrets internally and with other main third parties. These policies should be supported by detailed procedures demonstrating how the corporation's trade secrets are managed and highlighting many fields including data processing and detection, and usage of computers and personal devices at the corporation. Moreover, they stress the necessity of applying standards of security, such as the standards of information technology security (NIST Framework, COBIT, ISO 27001). The tools used for trade secret protection should be specifically designed on the system. In addition, information technology systems should be continually monitored and examined to ensure security and compliance with the usage requirements and secrecy of the corporation information [37]. The cybersecurity policies that should be applied by the business corporations include a risk management policy that focuses on two main objectives: identification and prediction of cyber incidents in order to be mitigated in the future, and presentation of a brief description for purpose, scope, and objectives of institutional risk management [39].
- **Roles and Responsibilities of Cybersecurity:** The cybersecurity is the duty of management that deals with all aspects of business at corporations. Therefore, every person belonging to the corporation should participate. However, to eliminate any confusion, there are main roles and responsibilities that should be played and assumed by every person within the cybersecurity system. The senior leadership should clearly assign roles and responsibilities to persons participating in the application of cybersecurity controls. The organizational structure of a corporation's governance and cybersecurity roles and responsibilities should be authenticated and approved, and competent persons should be assigned to perform the required duties. It is necessary to provide any support required for achieving duties, and attention must be given not to cause any conflict of interests [34].
- **Management of Cybersecurity Risks:** To make the cybersecurity governance program successful, business corporations should follow pioneering practices for risk management to implement a

program for protecting trade secrets by following a methodological approach. Moreover, the corporation's important assets, such as records of research, development, and strategic plans, should be given attention. The potential risks threatening trade secrets should be evaluated and examined as to how they can be taken, used, or disclosed with no permission. The reasons and ways leading to trade secret theft and enabling persons to commit such theft should be highlighted. The bodies contributing to trade secret theft may be persons inside a corporation, supply chain companies, employees, or external parties such as competitors and hackers [37].

- **Compliance and Control:** Cybersecurity governance is not only represented by plans, programs, and policies for protecting the corporations' cybersecurity, but it is an effort made to monitor compliance and continually perform measurement and improve [40]. Therefore, systems and processes should comply with a strict set of regulations and security requirements. Non-compliance should be encountered by specific regulations, big fines, and penalties [41].

2) Technology:

The technology tools, software and devices, are a very important factor to achieve effective cybersecurity for any corporation. An effective cybersecurity program should identify the cyber risks and select suitable measures and controls for reducing such risks.

The technology measures that should be taken by corporations to encounter, discover, and deter cyberattacks include the following:

- Preparation of an infrastructure for communications and information technology and enforcement of security standards that are internationally approved, such as the standard ISO 27001 for information security management
- Implementation of protective security tools: such as encryption, restrictive usage of internet [40], firewalls, intrusion detection system "IDS", and intrusion prevention system "IPS"
- Using antivirus and anti-malicious software programs
- Applying physical security measures and controlling login [42]

Security audit and intrusion detection play the most important role for business corporations. They ensure the quality of current cybersecurity controls and validate their effectiveness. In addition, security audit and intrusion detection are necessary to discover any intrusion affecting the corporation's system or network. Therefore, these two duties should be periodically and methodically implemented [18].

In addition, it is necessary to take security measures to secure cybersecurity data associated with how secret data are stored or transferred. Prevention of secret data transferring by applying restrictions on USB usage and electronic and physical distribution for protecting trade secrets should be considered [40].

3) Persons:

Capacity building seeks to spread knowledge of cybersecurity. It is associated with the human factor and has two main levels. The non-technicians should be aware of their important role in preventing and reducing cyberthreats. The effective implementation of employee awareness programs contributes to the identification of potential security problems.

It assists employees in understanding the cybersecurity consequences and ensuring the consistent application of procedures. Improving communication between teams and levels of corporations is also an advantage of employee awareness programs. However, technicians should have high skills, competencies, and qualifications for maintaining cybersecurity. Every corporation needs specialists to plan and implement the most complicated activities required to present an effective strategy for cybersecurity. Security department employees not receiving good training will not result in cybersecurity controls or the efficient management of risks. The corporation's capability to respond to cybersecurity incidents and recover from them will be based on technicians' efficacy [33].

A program for disseminating awareness and providing training for maintaining cybersecurity should be implemented [34]. Employees are the most vulnerable to security threats. They should be aware of any threats resulting from cyberattacks and sensitive data hacking to assist in protecting their corporation. All employees should be trained to ensure that they have the necessary security awareness and understand their responsibilities [41]. Moreover, they should have the required skills and qualifications, and they should receive training courses

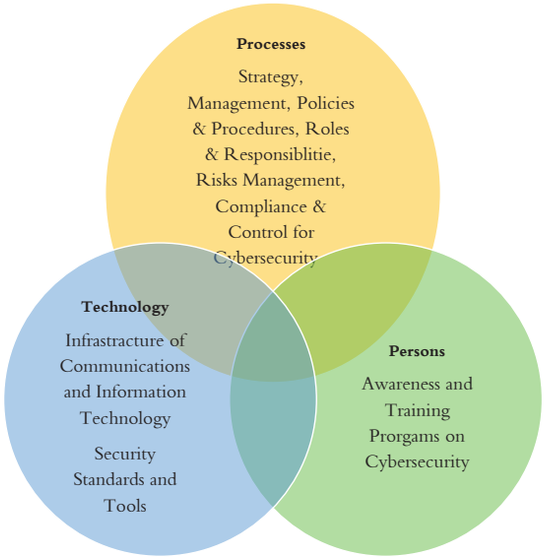

Fig. 2. Elements and Aspects of Cybersecurity Governance for Business Corporations

on cybersecurity to protect the corporation's digital assets and play their required roles [33]. Training and awareness of persons constitutes the bases to achieve cybersecurity governance for business corporations. Accordingly, a concept of the human factor of participation in protecting trade secrets and industrial intellectual property can be created.

Effective programs to increase employees' awareness and train them are a critical element in creating cybersecurity solutions. Educating employees is the best defense against threats of industrial cyber espionage. Employees have the responsibility of applying all the previous security solutions. Therefore, we can say that effective programs for awareness and training are an important requirement for sustainable cybersecurity.

From the abovementioned points, the roles of persons, processes, and technology are important in achieving success for cybersecurity governance programs characterized by coherence and adaptability. On the other hand, business corporations that have not realized the relationship between persons, processes, and technology will not counter the escalating cyber threats. Trying to prevent an attack will not be a solution; the business corporations should be ready to encounter and recover from potential cyberattacks.

The previous elements and aspects form a starting point for a positive contribution to redesign cyber governance by business corporations to achieve sustainable cybersecurity. Fig. 2 summarizes the elements and aspects of cyber security governance for business corporations.

C. Protection of Trade Secrets during Crises

The COVID-19 pandemic is considered one of the most critical challenges affecting all sectors. The current circumstances of this pandemic indicate that there are two types of business corporations:

1. Business corporations that are ready and have future plans to deal with any new events affecting business. They can remotely perform their duties.
2. Business corporations suffering from obstacles because they do not have suitable infrastructure and future plans for predicting risks that may negatively affect business and expose trade secrets and for dealing with threats that occur when transforming to enter the new environment of business. Therefore, such corporations must transform to meet challenges threatening the security and protection of sensitive information and trade secrets. Future plans should be prepared to deal with challenges and crises that suddenly arise and to assist business corporations in establishing a work system that has the capabilities to remotely work in a secure manner. Melman [43] sheds light on this point as follows:
    a. The Infrastructure Security: The security measures that should be taken by business corporations for protecting their computer networks

and infrastructures are based on a particular manufacture, information sensitivity, and authorized access, in addition to other factors that should be set and controlled. For example, accessing the corporation's secret information and trade secrets should be restricted to employees that need to perform specific duties. The corporation should secure the remote access systems, whether they are cloud-based share system, virtual private network "VPN", or any other way to remotely access the corporation's network. The business corporations must set administrative procedures to identify, report, and treat any breaches or unintentional leakage of secret information. Accordingly, procedures to reduce consequences and make suitable adjustments can be reconsidered. It is very important to take rapid action when discovering or doubting that sensitive information and trade secrets have been stolen.

b. Remote Security: The management of authorities is an important dimension for the security system of remote work. All managers working in information technology departments in corporations should employ tools and techniques for controlling users' access to important information. This access should be based on multi-level authentication for securing access management from unauthorized users [44]. Moreover, all employees who work remotely should be told how to take necessary precautions to maintain confidential information security. The corporation's secret documents and property should be handled and stored in case of remote work with the same level of attention given when working from the corporation's headquarters. The corporation should ensure that its employees are only performing their duties on devices assigned for work duties or on personal devices equipped with suitable and developed cybersecurity programs. All employees should also be directed to use business emails and electronic communications through addresses issued by the corporation. It is necessary to warn employees not to use public Wi-Fi networks when performing any secret transactions.

c. Social Media Policy: Many corporations encourage their employees to effectively use social media to improve communication and interaction with current or potential customers. Corporations use social media for marketing, but there are potential risks from intentional or unintentional disclosure of confidential information. These risks result from the low level of controls associated with social media usage. However, drafting and publishing social media policy to clearly guide employees to the permissible limits for discussing and handling confidential information and other sensitive information on social media is considered an important factor protecting the corporation's trade secrets.

V. Main Challenges Impeding Cybersecurity Governance Application in Business Corporations [35]

Cybersecurity is important for business corporations. Therefore, the study explores the most important challenges impeding the application of cybersecurity governance that must be identified and overcome by senior leaders. These challenges may be summarized as follows:

A. The Strategy and Objectives of Cybersecurity

The cybersecurity strategy will be a challenge for the corporation, unless its policies and objectives are clearly set. The logical sequence of the strategy's steps should be observed, i.e. the risk management approach should be set and followed before laying down the cybersecurity strategy. The risk evaluation should be made before creating a strategic plan for cybersecurity.

B. The Unified Processes

Task management is not always effective. Without approved and replicable unified processes, organizations can not ensure efficacy, quality, or consistency. Creation of replicable processes is an important factor for a corporation's comprehensive program of cybersecurity management. In brief, we can say that an ineffective cybersecurity program increases security breaches and cyberattacks.

C. Implementation and Accountability

The cybersecurity program will become inconsistent if governance requirements are neglected. Accordingly, a failure will occur. If requirements and processes are not clear, persons will set individual ways to perform work duties. This contradicts the unification of processes that constitutes a governance base for detecting the implementation of processes by employees. Cybersecurity governance should be measurable and practicable. The accountability principle should be applied to ensure employees' compliance with policies, procedures, and legal requirements. This approach can be implemented by continually monitoring how regulations are applied by employees.

D. Senior Leadership Control

Maintaining the effective management of cybersecurity is considered a main concern for corporations. Cybersecurity programs should be directed by senior leaders to ensure achievement of the processes' objectives. The corporation's efforts for managing risks will fail if the senior leaders do not support a sophisticated approach for cybersecurity governance. Moreover, the senior leaders should be aware of the life cycle of a cybersecurity governance program. Accordingly, cybersecurity governance programs can be highly supported and given due attention.

E. Resources

When senior leaders do not guarantee enough resources to satisfy the basic needs of cybersecurity governance, the high cost of such resources constitutes a critical challenge. The absence of compliance requirements related to funding a cybersecurity strategy suitable for a corporation is also a risk factor. Accordingly, secret information and information systems cannot be maintained or secured to counter various risks. Funding should also be specified for employees to be qualified and trained. In addition, appropriate tools for measuring key performance indicators should be bought to avoid any risks affecting replicable processes.

VI. Analysis of the Related Works

We can conclude that business corporations' dependence on cybersecurity governance programs is strongly associated with the sustainability of corporations' cybersecurity. It is obvious that governance ensures implementation of unified procedures and systems by senior leaders to be applied on all administrative levels and periodically monitored. The governance systems are flexible, as they can be provided with feedback for making continual improvement. The unified systems will be valid, even after changing management staff or human resources. The programs of cybersecurity governance grant the reasonable limit of basic aspects associated with trade secret protection. If such programs are violated, the efficacy of cybersecurity measures taken by the corporation will be reconsidered. The programs of cybersecurity governance constitute a security tool for acquiring loyalty of investors. They prove that the corporation has made efforts to maintain cybersecurity to actualize sustainable cybersecurity. American and international laws stipulate that legal protection granted for corporations' trade secrets is directly based on "reasonable procedures" taken by the corporation to protect information. Cybersecurity violations create escalating threats for corporations all over the world. The loss of a corporation's trade secrets may be devastating, as it will cause great damages affecting business, financial transactions, competitive advantage, and reputation [30]. Consequently, legal repercussions may arise. Vinnakota [9] applied a model for cybersecurity governance on a telecommunications institution in India. Such a model achieved many objectives such as countering cyberattacks against vital communications including email systems and online communications portals and dealing with cyber risks challenges affecting communication institutions. After applying the electronic form for diagnosis by surveying internal and external environments of cybersecurity, it was evident that the institution faced strong competition in the communications field. The important role played by a cybersecurity governance program for the board of directors and senior leaders was highlighted through meetings and workshops. Finally, based on the model, the board of directors implemented many procedures. By applying the cybersecurity governance model, the institution's systems and processes improved and cyberattacks were countered. This model proved its efficacy compared to traditional ways.

VII. Findings and Recommendations

A. Findings

- Advancements resulting from globalization and high dependence on information and communications technology have created a new mechanism

for industrial and economic espionage. Accordingly, espionage cases have increased, and their risks have escalated.

- Industrial espionage has clear indications that should be predicted to avoid risks. These risks result from the absence of a strategic cybersecurity plan, inefficacy of awareness and training programs on cybersecurity, and insecure infrastructure. Each indication includes some elements that should be given attention.
- Industrial espionage has negative effects on business corporations, including loss of market rank.
- Business corporations are subject to trade secret theft because technical, organizational, and social measures have not been taken.
- Governance contributes to corporations' sustainable cybersecurity by doing the following:
  - Activating the role of senior leaders in maintaining the corporation's cybersecurity
  - Providing leaders with a way to understand risk levels and precautions. Accordingly, incidents related to security breaches can be identified, encountered, and recovered.
  - The cybersecurity governance program prepares current and future plans for predicting any attacks resulting from industrial cyber espionage, in order to achieve sustainable cyber security.
  - The cybersecurity governance program includes plans, policies, laws, procedures, and awareness training programs. This contributes to business stability and corporations' sustainability in the long term.
  - Striking a balance between the security needs required for business corporations and expenditures
  - Identifying roles, responsibilities, and accountability to be employed as a measurement mechanism for reducing procedures interference
- The Integrated protection for business corporations cannot be achieved by technical measures alone. Rather, it requires organizational and social procedures applied under a unified frame adhering to the governance principle.
- The study indicates that the basic integrated elements processes, technologies, and persons are employed alongside the aspects of cybersecurity governance.
- The study highlights that business corporations are facing challenges when applying cybersecurity governance programs. These challenges are related to cybersecurity strategy, unified processes, implementation and accountability, senior leadership control, and resources.

B. Recommendations

- More specialized studies and research on the concept of cybersecurity governance and business corporations' ability to apply such a concept to actualize their objectives should be conducted.
- Business corporations should apply cybersecurity governance programs including the main elements processes, technologies, and persons covering sustainable cybersecurity aspects.
- The business corporations' senior leaders should follow the right methodology when applying cybersecurity governance. All steps should adhere to the logical sequence to avoid any challenges.
- The cybersecurity governance programs should be rapidly applied. Accordingly, the current world circumstances related to transition to remote work can be adapted.

REFERENCES

[1] V. Sridhar, "Cyber Security: A Two-Edged Sword!," in *Emerging ICT Policies and Regulations: Roadmap to Digital Economies,* Singapore: Springer Singapore, 2019, ch. 9, pp. 165-183.

[2] A. Jones, "Industrial espionage in a hi-tech world," in *Computer Fraud & Security,* vol. 2008, no. 1, pp. 7-13, Jan. 2008, doi: 10.1016/S1361-3723(08)70010-1.

[3] J. Arishee, "Sustainable Cybersecurity," (in Arabic), Dec. 22, 2019. [Online]. Available: https://makkahnewspaper.com//article/1500202/الرأي/الأمن-السيبراني-المستدام (accessed May 10, 2020).

[4] M. A. Al Thunibat, "Adapting to Cyber Risks," (in Arabic), 2019. [Online]. Available: https://althunibat.com/wp-content/uploads/2019/11/التكيف-مع-المخاطر-السيبرانية-للشركات-المالية-والائتمانية.pdf (accessed May 25, 2020).

[5] Brian Harrel, "Improving cybersecurity governance in the boardroom," Sep. 2017. [Online]. Available: https://www.

csoonline.com/article/3227887/improving-cybersecurity-governance-in-the-boardroom.html (accessed May 28, 2020).

[6] C. Konopatsch, "Fighting industrial and economic espionage through criminal law: lessons to be learned from Austria and Switzerland,"in *Security Journal,* vol. 33, no. 1, pp. 83-118, Mar. 2020, doi: 10.1057/s41284-019-00200-x.

[7] M. Sadok, C. Welch and P. Bednar, "A socio-technical perspective to counter cyber-enabled industrial espionage," in *Security Journal,* vol. 33, no. 1, pp. 27-42, Mar. 2020, doi: 10.1057/s41284-019-00198-2.

[8] I. Vasiu and L. Vasiu, "Cybersecurity as an Essential Sustainable Economic Development Factor," *European Journal of Sustainable Development,* vol. 7, no. 4, pp. 171-178, Oct. 2018, doi: 10.14207/ejsd.2018.v7n4p171.

[9] T. Vinnakota, "A Second Order Cybernetic Model for Governance of Cyber Security in Enterprises," *2016 IEEE 6th International Conference on Advanced Computing (IACC),* Bhimavaram, 2016, pp. 706-710, doi: 10.1109/IACC.2016.136.

[10] R. De Bruin and S. H. von Solms, "Cybersecurity Governance: How can we measure it?," *2016 IST-Africa Week Conference,* Durban, 2016, pp. 1-9, doi: 10.1109/ISTAFRICA.2016.7530578.

[11] A. Basuchoudhary and N. Searle, "Snatched secrets: Cybercrime and trade secrets modelling a firm's decision to report a theft of trade secrets," *Computer & Security,* vol. 87, Nov. 2019, doi: 10.1016/j.cose.2019.101591.

[12] D. Thorleuchter and D. V. D. Poel, "Protecting research and technology from espionage," *Expert Systems with Applications,* vol. 40, no. 9, pp. 3432-3440, Jul. 2013, doi: 10.1016/j.eswa.2012.12.051.

[13] M. Button, "Editorial: economic and industrial espionage," in *Security Journal,* vol. 33, no. 1, pp. 1-5, Mar. 2020, doi: 10.1057/s41284-019-00195-5.

[14] B. P. Gilbride, "Espionage – A Primer," in *The Professional Protection Officer,* 2nd ed, S. J. Davies and L. J. Fennelly, Ed, UK: Butterworth-Heinemann, 2020, ch. 28, pp. 321-330.

[15] H. K. Abdo, ala'oulmah walhyaah alyoumiah [Globalization and Daily Life] Egypt: The Anglo Egyptian Bookshop, 2011.

[16] K. Bissell, R. M. Lasalle and P. D. Cin, "Ninth Annual Cost Cybercrime Study," Mar. 2019. [Online]. Available: https://www.accenture.com/us-en/insights/security/cost-cybercrime-study (accessed Aug. 29, 2020).

[17] J. Clement, "Cyber espionage: most-targeted industries 2019," May 29, 2020. [Online]. Available: https://www.statista.com/statistics/221293/cyber-crime-target-industries/ (accessed Aug. 29, 2020).

[18] M. Khari, G. Shrivastava, S. Gupta and R. Gupta, "Role of Cyber Security in Today's Scenario," *in Detecting and Mitigating Robotic Cyber Security Risks,* R. Kumar, P. K. Pattnaik and P. Pandey, Ed, USA: IGI Global, 2017, ch. 13, pp. 177-191.

[19] B. Rothke, "Corporate Espionage and What Can Be Done to Prevent It," in *Information Systems Security,* vol. 10, no. 5, pp. 1-7, 2001, doi: 10.1201/1086/43315.10.5.20011101/31716.3.

[20] S. Bushwick, "How Iran Can Still Use Cyber and Drone Technology to Attack the U.S," Jan. 8, 2020. [Online]. Available: https://www.scientificamerican.com/article/how-iran-can-still-use-cyber-and-drone-technology-to-attack-the-u-s1/ (accessed May 30, 2020).

[21] A. Hamdy, "Learn about the most prominent cyber attacks of 2018 and 2019," (in Arabic), Nov. 30, 2019. [Online]. Available: https://jawalmax.com/learn-about-the-highlights-of-2018-and-2019-cyber-attacks/ (accessed May 25, 2020).

[22] G. Corera, "Coronavirus: Cyber-spies seek coronavirus vaccine secrets," (in Arabic), May 1, 2020. [Online]. Available: https://www.bbc.com/arabic/science-and-tech-52500415 (accessed May 31, 2020).

[23] M. J. Goldstein, *Cyber Attack,* 1st ed, Minneapolis, MIN, USA: Twenty-First Century Books, Aug. 2018.

[24] R. M. Stair and G. W. Reynolds, *Principles of Information Systems,* 13th ed, Boston, MA, USA: Cengage Learning, 2018.

[25] R. S. Mueller, "Combating Threats in the Cyber World: Outsmarting Terrorists , Hackers, and Spies," RSA Cyber Security Conference, San Francisco, CA, USA, Mar. 1, 2012. [Online]. Available: https://archives.fbi.gov/archives/news/speeches/combating-threats-in-the-cyber-world-outsmarting-terrorists-hackers-and-spies (accessed May 22, 2020).

[26] P. Binwal, "Creating a Cybersecurity Governance Framework: The Necessity of Time," June 29, 2015. [Online]. Available: https://securityintelligence.com/creating-a-cybersecurity-governance-framework-the-necessity-of-time/ (accessed May 19, 2020).

[27] C. P. Skroupa, "AN APPROACH 'ESSENTIAL TO CREATING ROBUST, SUSTAINABLE CYBER SECURITY'," Feb. 27, 2018. [Online]. Available: https://skytopstrategies.com/approach-essential-creating-robust-sustainable-cyber-security/ (accessed May 24, 2020).

[28] S. Boubaker and D. K. Nguyen, *Corporate Governance and Corporate Social Responsibility,* Singapore: World Scientific, 2015.

[29] T. Hawes, "Protect Your Company from Cyberthreats with Information Security Governance," July 31, 2018. [Online]. Available: https://mossadams.com/articles/2018/july/information-security-governance-as-a-cybersecurity (accessed 23, 2020).

[30] Infogouard, Information Security & Governance Solutions. [online]. Available: https://www.infoguardsecurity.com/cyber-se-

curity-governance-framework-development/ (accessed May 28, 2020).

[31] P. Passman, "Cybersecurity: Vital to Legal and Technical Protection of Trade Secrets," Feb. 12, 2017. [online]. Available: https://www.securitymagazine.com/articles/87807-cybersecurity-vital-to-legal-and-technical-protection-of-trade-secrets (accessed May 28, 2020).

[32] A. M. A. Al-Sartawi and A. Razzaque, "Cyber Security, IT Governance and Performance: A Review of the Current Literature," in *Implementing Computational Intelligence Techniques for Security Systems Design,* Y. A. Albastaki and W. Awad, Ed, Hershey, PA, USA: IGI Global, 2020, ch. 14, pp. 275-288.

[33] IT Governance, "A cohesive approach to cyber security." [online]. Available: https://www.itgovernance.co.uk/cybersecurity (accessed May 28, 2020).

[34] National Cybersecurity Authority, Aldawabit Al'asasiah lil'amn Alsybrani [Essential Cybersecurity Controls] Saudi Arabia: National Cybersecurity Authority, 2018. [Online]. Available: https://ega.ee/wp-content/uploads/2019/03/Essential-Cybersecurity-Controls.pdf

[35] S. Swinton, "Cybersecurity Governance, Part 1:5 Fundamental Challenges," July 25, 2019. [Online]. Available: https://insights.sei.cmu.edu/insider-threat/2019/07/cybersecurity-governance-part-1-5-fundamental-challenges.html (accessed May 15, 2020).

[36] Proactive Risk Management – The Key to Business Excellence. [Online]. Available: https://www.metricstream.com/insights/proactive-risk-management-approach.htm (accessed May 30, 2020).

[37] Protecting Trade Secrets from Cyber and Other Threats, 2018. [Online]. Available: https://thesedonaconference.org/sites/default/files/conference_papers/%5B3.1%5D%20CREATe.org_Protecting%20Trade%20Secrets%20from%20Cyber%20and%20Other%20Threats_2018.pdf (accessed May 27, 2020).

[38] AJ Kumar, "An Introduction to Cyber Security Policy." [Online]. Available: https://resources.infosecinstitute.com/cyber-security-policy-part-1/#gref (accessed May 27, 2020).

[39] H. Okonofua and S. Rahman, "Evaluating the Risk Management Plan and Addressing Factors for Successes in Government Agencies," 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE), New York, NY, 2018, pp. 1589-1592, doi: 10.1109/TrustCom/BigDataSE.2018.00230.

[40] P. Passman, "Protect your trade secrets using cybersecurity," Feb. 14, 2017. [Online]. Available: https://journal.iaccm.com/contracting-excellence-journal/protect-your-trade-secrets-using-cybersecurity (accessed May 22, 2020).

[41] J. Buddenberg, "CYBERSECURITY AND BUSSINESS SUSTAINABILITY," Nov. 5, 2019. [Online]. Available: https://www.moore-global.com/insights/articles/cybersecurity-and-business-sustainability (accessed May 22, 2020).

[42] L. Maglaras, M. A. Ferrag, A. Derhab, M. Mukherjee and H. Janicke, "Cyber Security: Form Regulations and Policies to Practice," in *Strategic Innovative Marketing and Tourism,* A. Kavoura, E. Kefallonitis and A. Giovanis, Eds, Cham, Switzerland: Spriner, 2019, pp. 763-770.

[43] D. J. Melman, "Protecting Trade Secrets During a Pandemic," Mar. 18, 2020. [Online]. Available: https://www.pearlcohen.com/protecting-trade-secrets-during-a-pandemic/ (accessed May 30, 2020).

[44] S. Shahidzedeh, "Why investing in identity access management is a must-do in a time of remote working," May 12, 2020. [Online]. Available: https://www.biometricupdate.com/202005/why-investing-in-identity-access-management-is-a-must-do-in-a-time-of-remote-working (accessed May 30, 2020).