[12]Horia AlQadhibi

A Conceptual Framework for Managing Cybersecurity Risks in Government Organizations

Journal of Electrical Systems

Abstract: - There is no doubt that cybersecurity risk management in government organizations is one of the main concerns of the governments worldwide. There are several concerns cybersecurity risk management across different organizations sectors, sizes ,and resources. In order to tackle the problems of diverse cybersecurity risks and purposefully risk management, it could be useful to assess and manage the different organizations' risk of cybersecurity. To achieve this ultimate goal, the researcher propose a conceptual framework for managing cybersecurity risks in government organizations. This framework considers three main dimensions for calculating risk metrics of (Information Technology) IT-assets in government organizations, which are vulnerability assessment, risk level measurements, and scoring of organization's risk profile. This framework could be used by researchers to develop tools for cybersecurity risk management and to recommend better security controls for improving risk management on government organizations.

Keywords: Risk Management (RM), Cybersecurity, Government organizations, Gordon–Loeb model, Axiom probability formula, Inherent risk formula.

I. INTRODUCTION

Government sectors around the world provide critical services to citizens with the aim of achieving sustainable development throughout the economy. They provides free electronic services to citizens, including medical, charity, judiciary, safety, and security services in a qualifying manner [1]. When we discuss government organizations, we are referring to the ministries, public institutions, and interest groups that offer independent public moral guidance [2]. They represent the backbone of their respective countries' national infrastructures. Therefore, many government organizations around the world has been experience by cyberattacks [3]. These attacks can vary from service disruptions ,data breaches and destroy of information technology infrastructure, which organizations should be protected from [4], [5].

Many cyberattacks result from a lack of experience among security practitioners about managing risks due to limited resources [6] . With the different cybersecurity risks that government organizations have suffered from recently [7], many governments grow worried about the security of their organizations' information , which increase the need for urgent solutions. This study introduces a conceptual framework for managing cybersecurity risks in government organizations. The organization of this paper is as follows: Sec. II includes background review about risk management in government organizations followed by Sec. III, which introduces the theoretical basis about risk metrics adopted in the framework. Moreover, section IV defines the suggested conceptual framework for managing cybersecurity risks in government organizations. Sec. V introduces an example of risk measurements according to the proposed framework. Finally, Sec. VI includes discussion and conclusion.

II. BACKGROUND OF CYBERSECURITY RISK IMANAGMANT IN GOVERNMENT ORGNIZATIONS

Cybersecurity is a multifaceted concept, which results in a multitude of cybersecurity definitions. The widely known view of cybersecurity is " the way of protect cyberspace from cyberattack " [8]. Cybersecurity risk could be defined as a measure of the extent to which an organization is a victim of an event and typically the outcome of a negative impact and the probability of occurrence. There are several concepts related to cybersecurity risk management that extend across different disciplines and debates, which cause confusion regarding the definition of risk. Table I presents the International Organization for Standardization (ISO) and the National Institute of Standards and Technology (NIST) definitions of risk management related concepts.

[1] *Corresponding author: Imam Mohammed Ibn Saud Islamic University, College of Computer& Information Sciences, Riyadh, Saudi Arabia

441022035@sm.imamu.edu.sa

TABLE I ISO'S AND NIST'S DEFFNITIONS OF CYPERSECURITY RISK ASSESSMENT CONCEPTS

Concept	ISO Definition	NIST Definition
Asset	Something valuable to the organization, such as IT infrastructure, intellectual property, experts, and consultants.	Items that have value to the organization.
Risk	A measure of the extent to which an organization is a victim of an event and typically the outcome of a negative impact and the probability of occurrence.	An abnormal event, which may have positive or negative effect on an organization.
Impact	The amount of harm from any violation to the organization's information system.	The result of an event affecting the organization.
Probability	Likelihood of a threat to or exploitation of a vulnerability.	The possibility of something happening.
Risk Assessment	The process of identifying, evaluating, and prioritizing risks resulting from the operation of an organization's information system.	Set of steps including risk identification, risk analysis, and risk evaluation.
Risk Identification	The process of determining and describing risks.	Set of activities to determine and describe risks.
Risk Analysis	The definition is the same as the ISO definition.	The process of recognizing the nature of and determining the level of risk.
Risk Evaluation	Comparing the outcome of the risk analysis for designing risk criteria to determine whether the size of loss is acceptable or tolerable.	The process of comparing the outcome of the risk analysis with the risk criteria to determine if the risk is acceptable or tolerable.
Risk Treatment	What take by an organization to modify risk.	Series of actions taken by organization to modify risk.
Security Controls	Its countermeasures include management, operational, and technical controls to protect of organization's information system.	Security measures that help in maintain risk.

With the increased number of cyberattack in government organizations , as mention by [7], the governments and the public sectors ranked first in terms of experiences with cyberattacks between April 2020 and July 2021 in Europe. Researchers found that many cyberattacks result from lack of experience among security practitioners about managing risks due to limited resources [6]. Furthermore, underestimating of asset value with poor investments in security technologies ,which lead to more expected risks [9]. The above review indicates that there is an extensive need for a precise assess and management of cybersecurity risks in government organizations.

III. RISK METRICS

Risk management is a challenging process because the cybersecurity risk problem has led to a security debate across different countries having diverse economic and religious statuses, rendering the choice of a suitable security protection level a problematical situation. To tackle this problem, the researcher incorporate between European Technology-supported Risk Estimation by Predictive Assessment of Socio-technical Security (TREsPASS) model and Saudi National Cybersecurity Authority-Essential Cybersecurity Controls (NCA-ECC) security controls as one cybersecurity risk management framework for government organizations, focusing on security risks from cyberspace. In this section, we will briefly introduce the theoretical basis about the adopted risk metrics and corresponding equations that we have used for building the blocks of the conceptual framework. We should emphasize that calculated metrics need to be interpreted for users with understandable recommendations.

A. Risk Identification

First, organizational assets and related threats should be identified using a socio-technical model as a modeling language with adopted of the attack tree notion to identify risk routes. The socio-technical model called TREsPASS is a collaboration project between government organizations and public sector institutions in Europe, aimed at helping organizations with large or complex infrastructures to represent their assets graphically [10]. In general, a trespasser means anyone with unauthorized access try to reach the IT-asset, whether physical or virtual. These threats are outcomes of interactions between the user and the technology. As such, the TREsPASS model is simple and easy to understand, even from people with limited knowledge on risk management. The model helps communicate and share security risk results visually to the risk manager which improve the monitor and management process. This model consists of six components: actor, asset, location, edge, policy, and process. Table II describes these main components. However, given our focus on attack initiated from outside the organizations and conducted through the cyberspace, the researcher will shed a spot light on five components out of six components ,which are actor, device, asset, policy, and connection.

TABLE II THE TREsPASS MAIN COMPONENTS

Components	**Descriptions**
Actor	Employee or group of employees sharing the same permissions, such as HR, IT, financial, etc.
Asset	All IT assets, including databases, software, servers, and networks.
Device	Every machine used to access the asset, such as desktop computers, laptops, tablets, and phones.
Connections	Represents the relation between actors who use devices to access the asset.
Policy	Security measures to which actors or devices have access to help minimize the probability of violations to the asset security.

After modeling the organization's IT-assets using these components, we assume the Connections between those components is fixed and represented as the Actor access the IT-asset through the Device. Some policy related to the Actor and others specific to the Device. By adopt the attack tree's notion, we can identify routes the attacker used to reach an asset. The attack tree is a graph-based approach that shows possible attack paths to the IT-assets. These paths are series of exploits steps that can be combined to initiate an attack target the IT-asset [11]. For example, the employee has access to the critical database via the device. If the employee get victim of an attack or the attack compromised his device, it should reach the critical database. Focusing will be on the risk is mutually exclusive events, which means if the attack target the employee, it should affect his device and vice versa. After mapping the organization's IT assets and determining the attack routes, the risk should be assessed, details of which will be discussed in the next subsections.

B. Risk Assessment

To calculate risk related to the IT-assets, we must first assess the probability and the impact of risk on the asset. Each employee with his device have an assigned estimated values ,which represents probability that an attacker will succeed in exploiting the employee or his device to harm an asset. According to [12],considering the symbol A as the probability of exploit the employee, and "B" as the probability of exploit his device, the probability to compromise the related IT-asset defined as in (1).

$$P(Asset) = P(Employee) + P(Device) - P(Actor * Device) \quad (1)$$

As mention earlier, the probabilities related to the employee and the device were pre-estimated values from cybersecurity experts, which are a decimal number in a scale from 0.0 to 1.0. The impact factor is reflecting the value of the asset in the organization, which is a scale from 0.0 to 1.0, where 0.0 reflect ineffective and 1.0 reflect critical. A more general equation to calculate risk level on the asset is presented in [6], where risk score is calculated

by computing the probability and the impact of the connected components. The risk level on asset calculated using (2).

*Risk= Impact * Probability* *(2)*

C. Risk Treatment

To enable a healthy organizational cyberspace presence, decision makers should realize the importance of security measures and try to investigate their security situations. The Gordon–Loeb mode is a well-known for calculating the effects of successful investments in cybersecurity on decreasing marginal returns [13]. To reduce overall risks on assets, we must first reduce the probability to exploit the connected components by apply the security measures or policy. In alignment with the Gordon–Loeb model, security measures have improvement on asset protection by decreasing the probability of component exploitation [14]. In using the Gordon–Loeb formula, the effect is the influence of security measures on improvements of the asset protection. The symbol I denotes the number of security measures applied to this component, and the symbol P denotes the probability of the component being exploited. The impact factor is a constant 0.80 value of the component, the effect of the security measure calculated according to (3).

$$Effects = 1 - \frac{impact\ factor}{(I+1)} \quad (3)$$

If their multiple security measures applied to the component, the probability to exploit the component will be calculated according to (4).

*P(component) = P(component) * Effects1* Effects2…Effects#* *(4)*

IV. CONCEPTUAL FRAMEWORK FOR RISK MANAGMENT

The results of the previous risk metrics enable defining a conceptual framework that integrates European TREsPASS model and Saudi NCA-ECC security controls of cybersecurity risk to give the organizational security practitioners ability to assess and manage the cybersecurity risk level. The risk metrics for risk management process that have been discussed in the previous section constitute the building blocks of the conceptual framework. An explication of our conceptual framework of managing cybersecurity risks on government organization is presented in Fig.1.

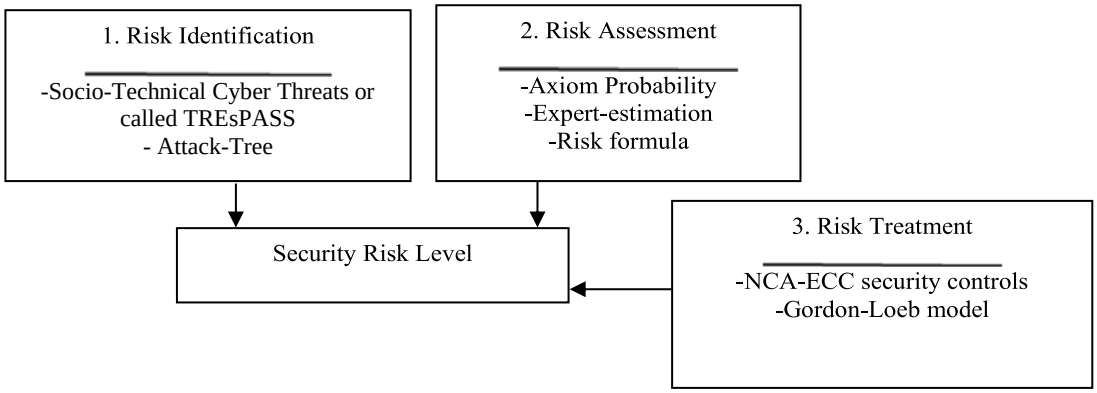

Fig. 1. *Conceptual framework of managing cybersecurity risks in government organizations*

Fig.1 show that the framework combines notions, theories and formulas in manage cybersecurity risk for governmental organizations. 1.Risk Identification using the TREsPASS model for modeling the organization's assets [10]. In addition to adopt of the attack tree notion to determine the risk routes to the IT-asset, referred to vulnerabilities [11]. 2.Risk Assessment by calculate the probability to exploit each component connected to the asset in accordance to the Axiom probability formula [12]. Considering the result of Axiom probability formula and the impact value , the security risk level calculated based on the Inherit risk formula [6]. 3.Risk Treatment based on the Inherit risk formula result, security risk level could be classified into one of the five risk scale categories. An example lustrates such calculation presented in the next section. One more value will be calculated which is the effect of security measure on the component (employee, device) exploitation. The used of the Saudi NCA-ECC as security measures and the Gordon–Loeb formula to calculate the effects of using more than one security measures

to reach an acceptable level of risks [14],[15]. Based on the conceptual framework in Fig.1, the classifying of different security risk level leads us to consider the following five-scale as shown in Table III.

TABLE III RISK SCALE AND CORRESPONDING RISK LEVEL

Legends		
Risk Scale	**Risk Level**	**Declarations**
0.00-0.10	Very Low	It is rare or may occur once in two years, and its impact is limited to the leakage of classified data (internal) within the organization.
0.11-0.30	Low	It may occur once yearly, and its impact is as low as the leakage of classified (confidential) data within the organization.
0.31-0.65	Medium	It may occur once every six months, and its effect is as medium as leaking classified data (internal) outside the organization.
0.66-0.89	High	The possibility of its occurrence is once every three months, and its impact is high, such as disabling a service or leaking classified (confidential) data outside the organization.
0.90-1.00	Very High	It is expected to occur monthly, and its impact is critical to the organization, such as the destruction of technical infrastructure or the leakage of classified (highly confidential) data outside the organization.

V. RESULTS

This example illustrates how different risk metrics in the framework could be used in assess security risk level. Let consider the following values as the results of applying equations of risk metrics on randomly selected risk scenarios yield from risk register for a jurisdiction government organization in Saudi Arabia. Table IV displays the results of security risk level for randomly selected risk scenarios.

TABLE IV RESULTS OF SECURITY RISK FOR RANDOMLY SELECTED RISK SCENARIOS

	Security Risk Levels	
Risk	**Before apply security measure**	**After apply security measure**
Leakage of cases database	0.74	0.48
Compromised the judiciary system	0.99	0.78
Unauthorized access to the Ethernet	0.74	0.48
Eavesdropping on pleading session.	0.77	0.50
Stealing of social media accounts	0.83	0.53
Breach of mobile application server	0.74	0.48

According to the given values, Compromising the judiciary system and stealing social media accounts are the riskiest to occur on the organization as show in Fig.2.

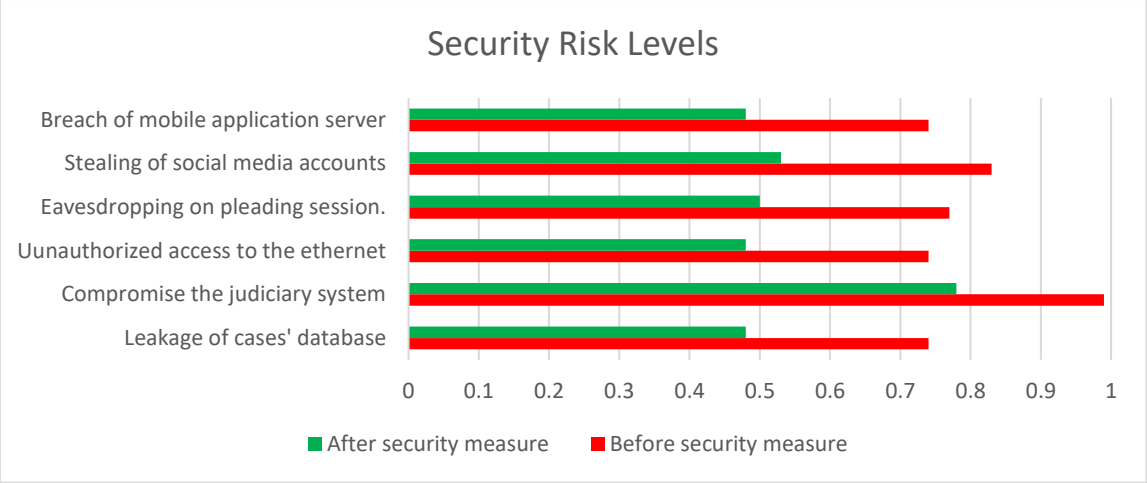

Fig. 2. *Different Security Risk Levels for Selected Risk Scenarios*

Emphasis will be on assets with high security risk levels for the next assessment to measure the effects of adding more than one security measure on asset security enhancement. Table V represents adding more than one security measures on minimize risk of Compromising the Judiciary System while Table VI represents adding more than one security measures on minimize risk of Stealing Social Media Accounts.

TABLE V Effects of Security Measures on Compromising the Judiciary System

Number of Security Measures Used	**Security Risk Level**
0	0.99
1	0.78
2	0.62
3	0.51

TABLE VI Effects of Security Measures for Stealing Social Media Accounts

Security Risk Level	**Number of Security Measures Used**
0.74	0
0.48	1
0.36	2
0.29	3

As declared in Table V and Table VI , respectively, each time a security measure is added, the security risk level decreases (even if it is small), For more enhancements, security practitioners will add more than one security measures until reaching an acceptable risk level. Both Fig.3. and Fig.4., respectively shows the differences in security risk levels when adding security measures on compromising the judiciary system and stealing social media accounts in a graphical format for better clarification.

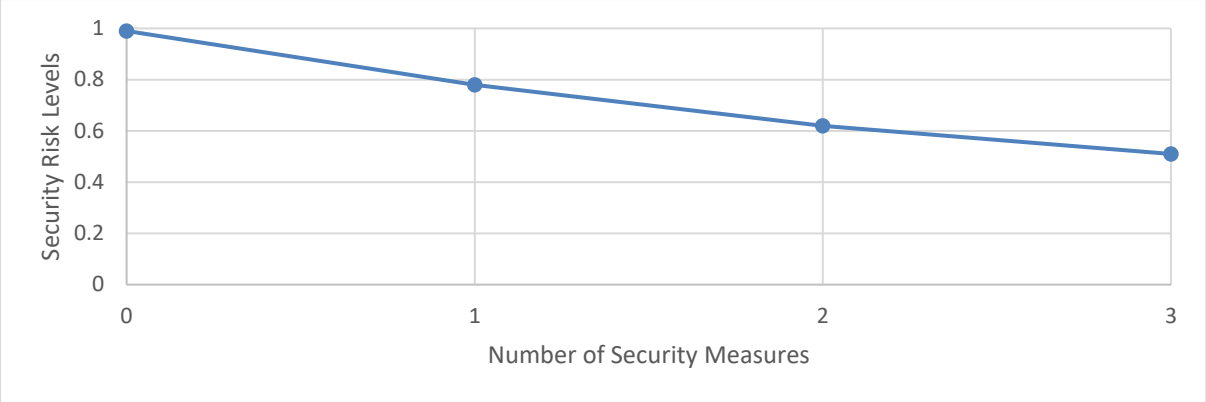

Fig. 3. *Effects of Security Measures on Compromising the Judiciary System*

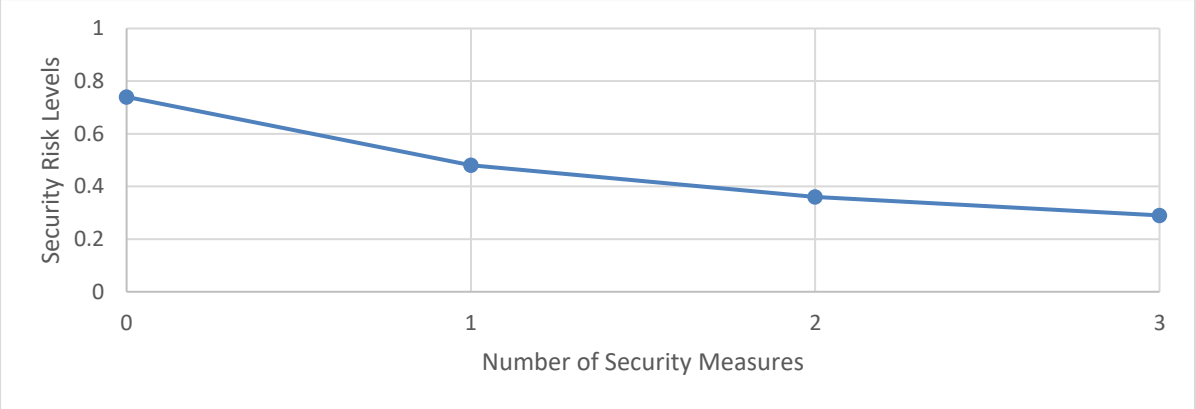

Fig. 4. *Effects of Security Measures on Stealing Social Media Accounts*

VI. DISCCUSSION AND CONCLUSION

Risk Management in government organizations is a challenging issue, especially with large organizations contains more than 300 employees with related devices and a list of permission to access the IT-assets. More and more expected risks, breaches, violations, and data exposures may happen, and efficient solutions are still inadequate and require great efforts.

In order to solve the problem of risk management , European TREsPASS model and Saudi NCA-ECC security controls could be combined together to constitute the risk management framework. This framework points to the importance of security practitioners' awareness of cyber threats and violations and its effect on organization security. It could be used as a theoretical basis for designing web-based tools or application for risk management. The work done in this research is a step forward and it considered a baseline that will shed light upon other security risks. The developed framework could be extended to other organizations that have issues in assess and manage their security risk. Furthermore, this study opens a new direction for integrates between National and International frameworks in order to provide solid basis in risk management, as this area has not yet gained wide adoption from researchers, and developers. We aspire to develop a comprehensive tool that enhances security practitioners' awareness of different security risks and employ the suggested risk metrics for better measurements.

A. Limitations

This study is limited by a small set of security risk scenarios .Although lack of a general risk scenario from other common data sources such as Saudi CERT, which is the common source for the government organizations.

B. Future Research

Other security risk such as physical attack can be investigated to assess and manage its impact on organization's security. In addition, taking advantage of Machine Learning algorithms in security risk severity prediction and take proactive steps toward managing and securing the organizations.

ACKNOWLEDGMENT

I would like to express my gratitude and special appreciation for Imam Mohammad Ibn Saud Islamic University represented by the College of Computer and Information Sciences and its professors. Appreciations are extended to all Information Systems faculty members of the department for their help throughout my study.

REFERENCES

[1] National Platform GOV.SA, A view for all governmental services, Retrieved August 25, 2023, from https://www.my.gov.sa/wps/portal/snp/servicesDirectory.

[2] Bureau of Experts,Government Nomenclature, Retrieved July 17, 2023, from https://www.boe.gov.sa/en/Translation/Pages/GovernmentLabels.aspx.

[3] Vaishy, S., & Gupta, H. (2021), "Cybercriminals' Motivations for Targeting Government Organizations," 2021 9th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions), ICRITO 2021. https://doi.org/10.1109/ICRITO51393.2021.9596104.

[4] Deora, R. S., & Chudasama, D. M. (2021), "Brief Study of Cybercrime on an Internet," Communication Engineering & Systems, 11(1), 7. https://doi.org/10.37591/JoCES.

[5] Morgan, S. (2020), Cybercrime To Cost The World $10.5 Trillion Annually By 2025. *Cybercrime Magazine*. https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021.

[6] DGA. (2022),"Risk Management for Digital Government ",Digital Government Authority. https://dga.gov.sa/en/Risk_Management_for Digital_Government.

[7] EuropeanParliament (2022)," Cybersecurity: main and emerging threats," 2022. https://www.europarl.europa.eu/news/en/headlines/society/20220120STO21428/cybersecurity-main-and-emerging-threats.

[8] NIST. (n.d.), *cybersecurity*. NIST. https://csrc.nist.gov/glossary/term/cybersecurity.

[9] Quadri, A., & Khan, M. K. (2019), CYBERSECURITY CHALLENGES OF THE KINGDOM OF SAUDI ARABIA. Global Foundation for Cyber Studies and Research (GFCyber). https://www.researchgate.net/publication/331009167_CYBERSECURITY_CHALLENGES_OF_THE_KINGDOM_OF_SAUDI_ARABIA .

[10] Coles-Kemp, L., Bullée, J.-W., Montoya, L., Junger, M., Heath, C. P., Pieters, W., & Wolos, L. (2015), *TREsPASS|Technology-supported Risk Estimation by Predictive Assessment of Socio-technical Security* (pp. 1–96). University of Twente. https://research.utwente.nl/en/publications/technology-supported-risk-estimation-by-predictive-assessment-of-.

[11] NCSC. (n.d.), *Risk management -Using attack trees to understand cyber security risk*. National Cyber Security Center (NCSC). Retrieved January 6, 2024, from https://www.ncsc.gov.uk/collection/risk-management/using-attack-trees-to-understand-cyber-security-risk.

[12] Stanford University. (n.d.), *The Axioms of Probability*. Retrieved October 28, 2023, from https://www.stanford.edu/search/?q=axoims+probability&search_type=web&submit=.

[13] Böhme, R. (2010), "Security metrics and security investment models,". Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 6434 LNCS, 10–24. https://doi.org/10.1007/978-3-642-16825-3_2/COVER.

[14] Gordon, L. A., & Loeb, M. P. (2002),"The economics of information security investment," *ACM Transactions on Information and System Security*, *5*(4), 438–457, https://doi.org/10.1145/581271.581274.

[15] NCA. (2018a), *Controls and Guidelines |Frameworks and Standards*. https://www.nca.gov.sa/en/legislation.