Contents lists available at GrowingScience

International Journal of Data and Network Science

homepage: www.GrowingScience.com/ijds

Cybersecurity effectiveness: The role of internal auditor certification, risk assessment and senior management

Budi Gunawan[a*], Barito Mulyo Ratmono[b], Denok Kurniasih[c] and Paulus Israwan Setyoko[c]

[a]Department of Cyber Intelligence, Sekolah Tinggi Intelijen Negara, Bogor, Indonesia
[b]Department of Technology Intelligence, Sekolah Tinggi Intelijen Negara, Bogor, Indonesia
[b]Department of Public Administration, Faculty of Social and Political Sciences, Universitas Jenderal Soedirman, Purwokerto, Indonesia

CHRONICLE

Article history:
Received: April 10, 2023
Received in revised format: May 18, 2023
Accepted: July 15, 2023
Available online: July 15, 2023

Keywords:
Internal Auditor
Cybersecurity
Risk Assessment
Senior Management Role
Internal Auditor Certification

ABSTRACT

This study aims to analyze and examine the influence of internal auditor certification, risk assessment, and the role of senior management on the effectiveness of cybersecurity for internal auditors who have experience in cybersecurity and information technology. This research method is a quantitative method, data analysis uses structural equation modeling (SEM) with SmartPLS 3.0 software tools. The population of this study is internal auditors who have experience in cybersecurity and information technology. The sample for this study was 480 respondents who were determined by the snowball sampling method. The research data was obtained from an online questionnaire which was distributed via social media. The questionnaire was designed using a Likert scale of 1 to 5. The stages of data analysis were validity test, reliability test and significance test. The results of this study indicate that internal auditor certification has a positive effect on cybersecurity effectiveness, risk assessment has a positive effect on cybersecurity effectiveness, and the role of senior management has a positive effect on cybersecurity effectiveness.

1. Introduction

In the current industrial era 4.0, almost all community activities are completely digital, and data is a very important and valuable resource in carrying out these activities, including e-commerce activities. If companies fail to overcome weak data protection, then it can become a serious threat to the company's business cycle. Gaps in the data protection system can lead to the emergence of various data security threats for companies. In addition to operational losses, these data security threats also have a negative impact on the company's overall image, especially when it comes to user data. Data security threats are getting more and more attention these days, increasing internet usage and weak data protection are the reasons why data security threats are on the rise. No one can guarantee the security of a system. Therefore, all parties involved in data-based activities must be prepared to anticipate and respond to data security threats. Data security threats are generally caused by cybercrimes. According to AlDaajeh et al. (2022) cybercrime is a criminal or irresponsible act committed by computer users who wish to take advantage of the widespread use of computer networks. This can certainly pose a serious threat to the integrity, security, and quality of most business information systems, and thus makes developing effective security methods a top priority (Mijwil & Aljanabi, 2023).

* Corresponding author.
E-mail address: baritoagp@gmail.com (B. Gunawan)

ISSN 2561-8156 (Online) - ISSN 2561-8148 (Print)

doi: 10.5267/j.ijdns.2023.7.011

According to Li et al. (2023) technological developments indirectly have an impact on the ease of dissemination of data and information. This increases the risk of cybercrime in the form of attacks to retrieve confidential data and reduces trust between customers and companies. Cybercrime will certainly create fear in the minds of many people who actively carry out e-commerce activities. Companies can know and record much information about customers. For example, home address, telephone number, account number, date of birth, and so on. The company can also record the history of purchases made by customers and compare it with the details of the remaining inventory in the company. Some forms of cybercrime that can generally occur in e-commerce are unauthorized access to computer systems and services, data alteration or theft, distributed denial of service attacks, online credit card fraud, phishing, vishing, and smishing. According to Khan et al. (2023), transactions carried out in e-commerce activities must be safe for sellers and buyers. When using the internet for transactions, trust is considered as an important and significant indicator. The openness of the internet which gives access to everyone can make the internet an open medium for carrying out cybercrimes. In addition, internet anonymity can hide the intentions of cybercrime actors, making it difficult to deal with cybercrime actions. Cybercrime has become a major concern worldwide. Many companies lose billions of dollars every year due to lost business, stolen assets, and damaged reputations due to cybercrimes. The bad impact of this cybercrime not only causes companies to lose a lot of money, but also lose their customers. This act of cybercrime can undermine the trust of merchants and customers in shopping online, which is considered an intangible loss. critical precautions are taken, and law enforcement is continuing to follow.

The industrial revolution is a process of fundamentally changing the way people live and work. The emergence of the industrial revolution 4.0 brought new changes in technological progress. The various impacts of these technological developments have greatly influenced people's behavior in carrying out economic activities (Li et al., 2023). Along with the increasing need for online markets, of course, this has resulted in various crimes. This crime does not only attack buyers and sellers, but store security is also very vulnerable to cybercrime attacks. Therefore, cases of cybercrime are classified as very high and often occur because some people try to take advantage of these crimes to fulfill their needs. According to Chaudhary et al. (2022), businesses in today's digital era, mostly focus on online business mode transaction activities and can build buying and selling activities with a better system by using a more humane relationship and having personalization with customers without relying on things whatever.

In the era of the industrial revolution 4.0, all aspects of life are inseparable from the touch of technology, driving digital transformation of activities and business processes in various sectors. This gave birth to a variety of technological innovations such as Artificial Intelligence and the Internet of Things (IoT). According to Masoud and Al-Utaibi (2022) the role of IoT technology also results in Cloud Computing and Big Data. Through the development of information technology, every device is now easily connected to computer networks such as the internet. According to the World Bank, based on ITU (International Telecommunication Union) data, the portion of internet users in the world was around 49 percent of the population in 2017, this portion increased rapidly compared to 2000 which was only around 6.7 percent. Similarly, Internet World Stats estimates that the portion of internet users in the world will be 64.2 percent of the population in the first quarter of 2021. The estimated number of internet users is more than 5 billion, this number has increased by around 1,300 percent compared to 2000. The increase in the number of internet users in the world is inseparable from the increase in the number of threats or cyber-attacks (Mijwil & Aljanabi,2023). Indonesia recorded that in 2018 there were 12.8 million attacks. In 2019 there were 98.2 million attacks, then in 2020 there were 74.2 million attacks. Like the story of an impenetrable shield and a spear that can penetrate anything, cyber-attacks continue to create potential threats to the system all the way to the end-user. In 2021, several parties believe that cyber-attacks will not subside. Kaspersky, for example, stated that the COVID-19 pandemic could create various waves of poverty which are likely to increase crime, including carrying out cyber-attacks. One solution to minimize this is to pay attention to the management of cybersecurity systems. According to Shillair et al. (2022) cybersecurity is much needed protection for individuals, companies, or governments to protect and prevent misuse of access to and utilization of data in information technology systems from someone who does not have the right to access or utilize data in the system.

According to the Minister of Communication and Informatics, in 2023 the increase in the use of information technology, such as the internet, will increase by 44 percent, but with the increase in the use of information technology, it will have an impact on increasing cybersecurity. According to the National Cyber and Crypto Agency (BSSN), there have been 888,771,736 cyber-attacks in Indonesia recently. Cyber-attack incidents can consist of several types of events such as malware, ransomware, card payment fraud and internal errors. The ever-changing nature of cyber-attacks, for that every company and business at the cybersecurity level must be increased. According to Khan et al. (2023), cybersecurity and information security are in the top two rankings of technological risk problems faced by companies. Lim et al. (2023) revealed that as many as 570 Chief Audit Executive (CAE) supervision was carried out by the European Confederation of Institute of Internal Auditors (ECIIA), cybersecurity is ranked in the top 5 (five) in business risk. AlDaajeh et al. (2022) revealed that cybersecurity audits are a new practice in security to support asset protection company information, in the audit process to obtain evidence of the organization's information security policies and effectiveness to protect asset integrity, data confidentiality, and access data availability. Internal audit has an important role to play in assisting organizations in managing cyber threats, by providing an independent assessment of its controls where needed and helps audit committees and boards understand and address the risks of the digital world.

A security or cybersecurity audit requires sophisticated information technology knowledge, internal auditors must have sufficient knowledge of the main IT risks and control available technology-based audit techniques. An internal audit that has information technology knowledge such as having a certification means that a high-quality security audit such as a Certified Information System Auditor (CISA) and Certified Information Security Manager (CISM). Effective first step for internal audit by conducting a cyber risk assessment and summarizing the findings into a summary for audit committees and boards which will then drive a risk-based cybersecurity internal audit plan. According to Victory et al. (2022) and Wu et al. (2022), activities, the most important in cybersecurity assessments, are identifying the most valuable digital assets. The practice of assessing risk varies widely across organizations. Kurniawan et al. (2023) revealed the role of senior management in improving cybersecurity by reviewing information technology security design, planning and development of information security policies accompanied by successful implementation and senior management commitment can play an important role in instilling a level of information security culture that leads to the establishment of a framework. Chaudhary et al. (2022) revealed that the strategy adopted by senior management is said to be effective if well-developed and interrelated strategies are spread throughout the company, in carrying out the strategy supported by information technology governance to ensure the implementation of planning and development of information security policies and security procedures. According to Oumaima et al. (2022) companies invest in technology to improve security to prevent possible victims of cyberthreats. Technical measures can include both proactive security and reactive security. Proactive security includes digital signatures, cryptographic keys, digital certificates, antivirus, and anti-phishing scanners. Reactive security includes access control techniques, firewalls, passwords and remote access, biometrics, and intrusion detection systems. Shillair et al. (2022) revealed that failures in information technology (IT) systems can increase cyber risk across organizational networks, therefore information technology managers are more vigilant in choosing software with uncorrelated vulnerabilities when building system configurations.

2. Literature Review and Hypothesis Development

2.1 Internal Auditor Certification

According to Masoud and Al-Utaibi (2022) internal audit is an independent activity, providing assurance and consulting designed to provide added value and improve organizational operations. CIA is a certification given to the profession of internal auditors and issued by the Institute of Internal Auditors (IAA) Florida, United States of America. The exam system is usually conducted online. In Indonesia, the institution that issues this certification is the Internal Audit Education Foundation (YPIA). Internal auditing assists organizations in their efforts to achieve their goals by providing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and organizational regulatory and management processes. According to Nyre-Yu et al. (2022), to become a certified internal auditor (CIA), the individual must pass an examination and have a minimum of two years' work experience as an internal auditor or equivalent. Criteria for internal audit experience includes experience in public accounting. To earn a CIA certificate, an individual must follow the standards of practice and code of ethics from the IIA as well meet continuing professional education requirements. The CIA doesn't need to be authorized by a government agency (Mijwil & Aljanabi, 2023).

2.2 Risk assessment

Risk assessment is a process carried out by an agency or organization and is an integral part of the risk management process in making risk decisions by carrying out the stages of risk identification, risk analysis, and risk evaluation. The risk management process refers to the ISO standard 31000: 2018, can be grouped into the determination stage: (1) scope, context, and criteria, (2) risk assessment, and (3) risk treatment stage. Stage 1, namely determining the scope, context and criteria has been described in the previous article. This article will describe risk assessment, as a follow-up stage after stage 1 is compiled. In general, risk assessment is the entire process of risk identification, risk analysis and risk evaluation. According to Selimoglu and Saldi (2023), risk assessment is basically an activity of assessing the possibility of events that threaten the achievement of organizational goals and objectives. Risk assessment must be carried out systematically, iteratively, and collaboratively, by utilizing the knowledge and views of stakeholders. Risk assessment must use the best available information, complemented by further observations as needed. The risk assessment process consists of three elements, namely (1) risk identification, (2) risk analysis, and (3) risk evaluation. Methods that can be used at the risk identification stage include checklists, consideration based on experience and documents, benchmarking, flow charts, brainstorming, system analysis, scenario analysis. FGD, interviews, document review, observation, SWOT analysis, Event Tree Analysis, and surveys & questionnaires. According to Wylde et al. (2022), a comprehensive risk assessment is a combination of qualitative and quantitative assessment methods. The stages of risk evaluation include: (1) compiling risk priorities based on the amount of risk provided that: a) the highest level of risk gets the highest priority. b) If there is more than one risk with the same risk magnitude, the risk priority is determined based on the sequence of impact areas from the highest to the lowest according to the impact criteria. c) If there is still more than one risk that has the same magnitude and area of impact, then the risk priority is determined based on the order of the highest to the lowest risk category according to the risk category. d) If there is still more than one risk that has the same magnitude, area of impact, and category, then the risk priority is determined based on the judgment of the Risk owner (Wissink et al., 2023).

2.3 Management Role

The role of management in the company is very important, namely, to ensure that everything related to achieving goals can be carried out successfully. Without a plan, then what to do? Therefore, the most important step in company management is planning. This is important in determining the goal, direction, and orientation of the company. According to Shillair et al. (2022) there is not only one plan, but also what is called an annual plan, a long-term plan, a medium-term plan, and a short-term plan. The task assignment process is also an important part of company management. With such a big plan, a manager must be good at dividing and placing each worker into each task concerned. After assigning each task to the right members, briefings are made for more focused company management. In directing, managers must be detailed and precise so that it can be clearly understood by company workers. This will later become the starting point for the company's missions. After planning, placing and directing are given, managers must be proficient in supervising or supervising each part of the worker. Scheduled and directed oversight will bring missions that 'strike' or 'misdirected' back on the right track. and supervision in accordance with the delegation of responsibilities for each existing human resource.

2.4 The Effect of Internal Auditor Certification on Cybersecurity Effectiveness

Nyre-Yu et al. (2022) stated that an internal auditor must have knowledge of the system to assist management in making decisions. Every individual who has the responsibility in assessing cybersecurity must have knowledge of information system audit techniques and information security standards and suggest values for professional certification in this field. The existence of certification and training programs can form capacity building for human resources in the field of cybersecurity, which is useful for improving cybersecurity in Indonesia, even though Indonesia does not issue certification, accreditation of national and professional institutions regarding cybersecurity, but professionals in the field of cybersecurity have held a professionally recognized cybersecurity certification.

H$_1$: *Internal auditor certification has a positive impact on cybersecurity effectiveness.*

2.5 Effect of Risk Assessment on Cybersecurity Effectiveness

The purpose of risk assessment is to be able to find out the status of these risks and identify how to deal with this risk. Cybersecurity is a major component of audit risk assessment. Cybersecurity risks are mandatory on information technology risk assessment, it will be a component of audit risk assessment overall which has proven that risk assessment has a positive effect on security/cybersecurity audits.

H$_2$: *Risk assessment has a positive impact on cybersecurity effectiveness.*

2.6 The Influence of Senior Management Role on Cybersecurity Effectiveness

The management and the board of directors have the power and responsibility to ensure the company's top priorities, to ensure the scope of security, resilience as a priority and must be communicated within the company. Senior management monitors privacy risks in situations like cybersecurity risks, financial risks and other organizational risks. Senior management's role in cybersecurity by reviewing information technology security design, security implementation and retrieval strategic decisions, as well as the establishment of a security governance framework.

H$_3$: *Senior management role positively influences cybersecurity effectiveness.*

3. Method

This research method is a quantitative method, data analysis uses structural equation modeling (SEM) with SmartPLS 3.0 software tools. The population of this study is internal auditors who have experience in cybersecurity and information technology. The sample for this study was 480 respondents who were determined by the snowball sampling method. The research data was obtained from an online questionnaire which was distributed via social media. The questionnaire was designed using a Likert scale of 1 to 5. The stages of data analysis were validity test, reliability test and significance test. empirical study accompanied by statistical data, characteristics and patterns of relationships between variables. This study uses hypothesis testing which aims to explain and test the influence of independent variables, namely internal auditor certification, risk assessment, the role of senior management, strategies adopted by senior management and technical steps in improving cybersecurity on cybersecurity as a variable. dependent. The data used in this research is primary data which is a source of research data obtained directly from the original source, the data source is obtained directly from internal auditors who are experienced in the field of cybersecurity and information technology. The time of data collection in this study was cross-sectional, which is data whose observations were made at one time with many objects at the same time. This study used a sampling method, namely non-probability sampling using the snowball sampling method. In this study the size of the population cannot be determined because the population is unknown. In this study conducted through a questionnaire. The survey was conducted by distributing questionnaires in the form of a Google form link online. The questionnaire contains statements to respondents, namely internal auditors who oversee evaluating cybersecurity in companies or internal auditors who use information technology. Fig. 1 shows the structure of the proposed study.

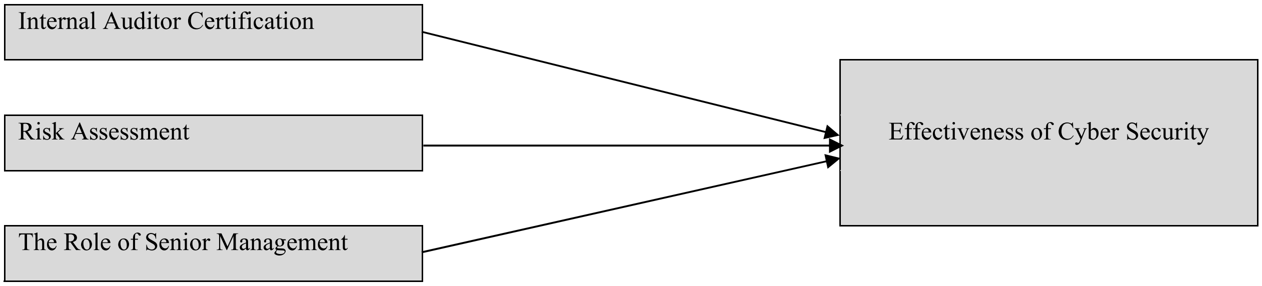
Internal Auditor Certification
Risk Assessment
The Role of Senior Management
Effectiveness of Cyber Security

Fig. 1. Research Hypothesis

4. Result and Discussion

4.1 Partial Least Square (PLS) Analysis

Outer Model Test The outer model is a model that specifies the relationship between latent variables and their indicators, or it can be said that the outer model defines how each indicator relates to its latent variables. The outer model is interpreted by looking at several things, including convergent validity values, discriminant validity values, composite reliability, Average Variance Extracted (AVE) and Cronbach's alpha. a) Convergent validity: The convergent value is measuring the magnitude of the loading factor for each construct. a loading factor above 0.70 is highly recommended, however a loading factor between 0.5 - 0.60 can still be tolerated if the model is still in the development stage. The PLS Algorithm model and the complete indicator loading value. After the Outer loading test is carried out, the outer loading value is obtained in the table above. The table above shows that all indicator values have met the requirements, namely > 0.70.

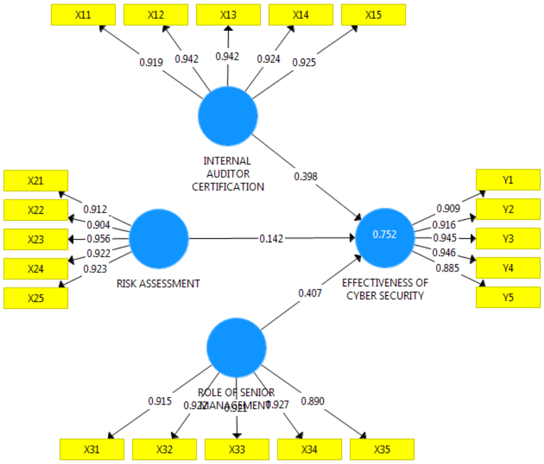

Fig. 2. Validity Testing

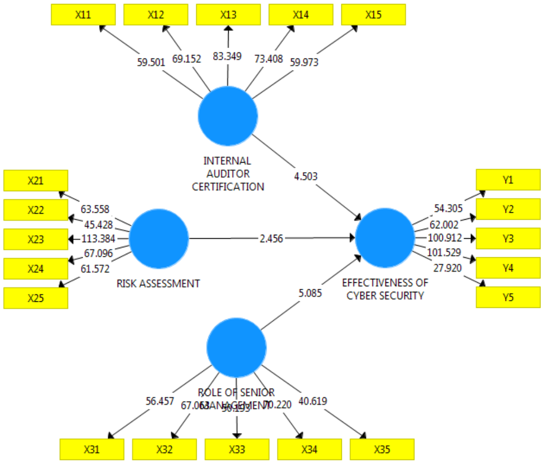

Fig. 3. Hypothesis Testing

4.2 Reliability and Validity

As shown in Table 1, all values of Cronbach's alpha, composite reliability, and rho-A are well above the threshold of 0.70 (Hair et al., 2012; Purwanto et al., 2023). These results signify that the constructs are reliable and performed well. AVE for each construct is above 0.50, indicates theconvergent validity. Finally, all the VIF values are less than 3, establishing the lack of multi-collinearity issues among the study constructs.

Table 1
Reliability Analysis

Variables	Cronbach'sAlpha	Composite Reliability	Average Variance Extracted
Internal Auditor Certification	0.832	0.815	0.732
Risk Assessment	0.826	0.854	0.715
Role of Senior Management	0.832	0.815	0.624
Effectiveness of Cybersecurity	0.834	0.821	0.624

Hypothesis Testing a) Direct Influence Analysis Whether or not a proposed hypothesis is accepted, it is necessary to test the hypothesis using the Bootstrapping function on SmartPLS. The hypothesis is accepted when the significance level is less than 0.05 or the t-value exceeds the critical value. Or the t statistics value for a significance level of 5% if the t-statistic value is > 1.96 then the null hypothesis (H0) is rejected. The results of the PLS Bootstrapping Model are presented in Fig. 3.

Table 2
Hypothesis Testing

Hypothesis	Coefficient	t- values	Sig	Decision
Internal Auditor Certification on Cybersecurity Effectiveness.	0.398	4.503	0.000	Supported
Risk Assessment on Cybersecurity Effectiveness.	0.142	2.456	0.000	Supported
Senior Management Role Cybersecurity Effectiveness	0.407	5.085	0.000	Supported

Based on the picture and table above, the interpretation of the research hypothesis is as follows:

First hypothesis: The effect of auditor certification on cybersecurity effectiveness

From the results of statistical testing t, the value is 0.956, which means that internal auditor certification such as CISA and CISM has a positive effect on the effectiveness of cybersecurity and seen from a significance value of 0.0155 <0.05, Ho is rejected so that it is statistically proven that internal auditor certification has an effect significant positive effect on the effectiveness of cybersecurity. According to Oumaima et al. (2022), Parker et al. (2023), Sam et al. (2022) and Slapničar et al. (2022) more than 90 percent of cyber incidents in cyberspace are caused by user negligence due to a lack of understanding of internet security, such as an employee leaving his computer unlocked. For this reason, training and outreach are needed to increase internet awareness.

Second hypothesis: The effect of risk assessment on cybersecurity effectiveness

From the results of the statistical test t, the value is 0.519, which means that the risk assessment has a positive effect on the effectiveness of cybersecurity and seen from a significance value of 0.01 <0.05, Ho is rejected so that it is statistically proven that the risk assessment has a significant positive effect on the effectiveness of cybersecurity. According to Masoud and Al-Utaibi (2022), Nyre-Yu et al. (2022) and Shillair et al. (2022) organizations must protect networks using firewalls, facilitate the development of data filtering rules according to organizational security standards, ensure the security of user passwords, change passwords periodically and ensure that only employees use computers connected to the network. Organizations can use special Wi-Fi for guests, the device is set to automatically lock if it is not used for three minutes, using the lock screen automatically.

Third hypothesis: The effect of senior management on security effectiveness cyber

From the results of the statistical test t, the value is 0.303, which means that the role of senior management has a positive effect on the effectiveness of cybersecurity and seen from the significance value of 0.0075 <0.05 then Ho is rejected so that it is statistically proven that the role of senior management has a significant positive effect on effectiveness cybersecurity. According to Parker et al. (2023), Sam et al. (2022) and Slapničar et al. (2022) the role of senior managers ensures that employees and all parties comply with data security procedures, all employees, contractors, and guests must accept and have read data security procedures.

Strategy is the process of establishing the company's vision, organizational goals, formulating certain policies and ways to achieve goals and ensuring proper implementation so that organizational goals and objectives will be achieved. According to Masoud and Al-Utaibi (2022) security policy refers to instructions on maintaining security. The strategy adopted by senior management to improve cybersecurity in the organization by establishing a clear vision can establish measurable information technology security goals, evaluate information security systems, security risk management and share information on security technology. Masoud and Al-Utaibi (2022) and Shillair et al. (2022) state that to implement security policies and standards, it is necessary to follow a guide to practice procedures which include practical guidelines and steps. With senior management working with the auditor to establish policies regarding security measures and objectives, efficient organization and probability. It is the auditor's responsibility to evaluate the procedures to be included and include cybersecurity measures in the list of audit activities. Policies and strategies regarding system development and procurement, technology operations information, communication networks, information security, and disaster recovery plans. Security managers taking cybersecurity precautionary measures in the organization will have an impact on the cybersecurity environment, with proactive information security measures and enterprise technical measures can improve cybersecurity in the enterprise (Wissink et al., 2023).

The digital era makes people feel comfortable in various aspects of life, including in the business world. Online transactions have become commonplace and almost everyone does it. However, this is also accompanied by cyber threats that have the potential to harm users. Risks such as data theft, access to sensitive information to the destruction of important data must be considered by every business person to ensure the security of customer data (Kemp, ,2023). The existence of e-payments in digital payment transaction systems, which are currently becoming a trend, is not an exception, in fact it should be a major concern for business people. The risk of data leakage and embezzlement of digital account balances is enough to be a big threat. This is where cybersecurity becomes important to be implemented in all online transaction systems. Cybersecurity is the act of protecting devices, networks, programs and data from the threat of cyber- attacks and illegal access. With cybersecurity, the risk of losing a user's balance and personal data can be minimized (Arpaci & Aslan, 2023).

The cybersecurity system is basically divided into three types, namely: 1. Network Security is a security system that protects data traffic among an increasing number of users through increased network security. The existence of network security is considered effective in protecting company assets and maintaining network data traffic. Several methods for activating network security include installing antivirus, firewalls, two-factor authentication, and data encryption. 2. Cloud Security, Cloud-based services are now widely used by users to store important data. But unfortunately, this cloud computing system is still vulnerable to attacks from hackers, so now the cloud security campaign has become intense (Wylde et al., 2022). Cloud security threats are usually anticipated by installing a firewall, two-factor authentication, and data encryption. 3. Application Security, e-business currently does not only rely on websites as a means of communicating with customers, but also with self-made applications. This application is expected to make it easier for customers to access and get the latest information about a product. This is the importance of application security to prevent the risk of data theft. Application security is usually in the form of authentication, both biometrics and identity cards (Eboibi & Ogorugba, 2023).

Cybersecurity is the right solution to prevent cyber-attack threats. In fact, there are three cybersecurity threats, each with a different outcome. 1. Cyber-attacks, cyber-attacks are usually in the form of attacks on companies or political interests. Cyber-attacks are often carried out with the excuse of creating riots and seeking profit (Steinmetz et al.,2023). But that does not mean that cyber-attacks only aim to pit one against the other. Some victims unknowingly even experience data theft and misuse. Cybercrime, cybercrime is a type of crime that includes illegal transactions, destruction of computer systems and manipulation of data. The main motive of cybercrime is usually material. Even so, there are several hackers who use cybercrime methods with the aim of causing chaos. Cyber terrorism, cyber-attacks that are continuously occurring causing excessive fear and creating mass panic can be classified as cyber terrorism. The emergence of cyber terrorism usually begins with a similar pattern, namely spreading fear so that people feel confused and panic about the steps that must be taken immediately (Nwankpa et al., 2023).

Cybersecurity is an action to protect computer systems from digital attacks or illegal access. There are several elements of cybersecurity, including application security, information security, cloud security, network security, disaster recovery/business continuity planning, operational security, and end-user education. These elements are critical to ensuring overall cybersecurity security, as the risk of exposure to digital threats continues to increase and the threats are increasingly diversified (Kemp, ,2023). Therefore, it is important to protect the system from even the smallest risks. There are also types of cyber threats based on the mode of operation of their implementation, namely: Cyber Crime, In the practice of cybercrime, perpetrators make illegal access such as illegal transmission or manipulation of data for specific purposes, including creating disturbances and seeking financial gain, can be done alone or involve a group of people. The perpetrators of cybercrime are certainly people who are experts in various hacking techniques, it is not uncommon for cybercrime to be carried out from various places at the same time. There are many examples of cybercrime that still occur, such as identity theft, credit card fraud/theft, spying on certain targets (cyber espionage), and others. Every crime in cyberspace, of course, results in losses for the victims, the losses resulting from cyber-attacks are also very large (Kumar et al.,2023). The potential for economic losses in Indonesia caused by cyber-attacks has resulted in losses reaching IDR 478.8 trillion or US$34.2 billion. The value of these losses is more than 3 percent of Indonesia's GDP in 2018. Implementing effective cybersecurity is now a challenge because there are so many devices compared to users, and attacks are becoming more innovative. Although the supporting infrastructure for cybersecurity has been strengthened recently, this does not rule out the possibility of an exponential increase in cybersecurity threats (Creemers et al., 2023).

Various forms of cybercrime are often used by perpetrators among them in the form of e-mail spoofing, which is forgery of e-mail headers. Received e-mail messages appear to have been sent by genuine, actual, and trusted sources. This mode is usually used in spam or phishing campaigns. The target may open the e-mail thinking that the e-mail has been sent by a legitimate source (Utomo et al., 2023). Hacking is a covert breach of a computer system and stealing valuable data from the system without permission. The spread of a virus or malware is a collection of cyber instructions that can carry out some malicious operations. Viruses and malware stop the normal functioning of system programs and insert some abnormalities from the performance of the affected system. Viruses and malware can spread via email, chat messages, data stores, multimedia, internet, and other electronic media. Phishing is an act of stealing personal information such as passwords, credit card details, user data targeted victims via the internet. This form of cybercrime is carried out by spoofing emails and instant messages to victims. The hacker creates a direct link that directs the targeted victim to a fake website page that looks identical to the real website (Pratiwi et al., 2021).

According to Parker et al. (2023) the risk of cybercrime that takes advantage of cybersecurity gaps in fintech is an entry point for cybercrime so that appropriate cybersecurity measures are needed with the following actions: a. Protect and monitor wireless access points, network access points, and network-attached devices with a layered security system and control all user access to information resources. b. Control and limit internal user access rights to files or data only that relate to job tasks. c. Prevent and secure all users and system managers who are targeted by cybercrime. d. Authentication in virus, trojan, malware and other malicious programs. e. Perform periodic scans using an antispyware program to detect spyware, adware and bots (software robots) and other malicious programs. f. Provision of education and training on awareness of the importance of security and caution in using internet services. Cybercrime is a necessity that will continue to exist along with the rapid development of information and communication technology, so that reliable and effective cybersecurity is needed to deal with it. The challenges of cybercrime in fintech include weak cybercrime regulations, data and information theft and intellectual property theft that impact fintech's reputation. To mitigate the cybercrime challenge, cybersecurity is required through proactive actions, strengthening regulations and establishing a reliable, effective and efficient cybersecurity framework or procedure. According to Slapničar et al. (2022) most cybercrime victims are e-commerce users or actors, namely buyers and sellers. Thus, this can be considered as an important note about the level of awareness of the Indonesian people about cybersecurity.

5. Conclusion

Based on the results of the study we can draw different conclusions. Based on the results of the analysis, internal auditor certification has maintained a positive and significant relationship to the effectiveness of cybersecurity. Based on the results of the partial influence analysis, the risk assessment variable has also made a positive and significant relationship to the effectiveness of cybersecurity. Moreover, based on the results of the partial influence analysis, the management role variable has a positive and significant relationship to the effectiveness of cybersecurity. To increase the effectiveness of cybersecurity for internal auditors, internal auditor certification, risk assessment and senior management role support are required, therefore internal auditors need to apply for certification, make risk assessments and get full support from senior managers. The research produced a relationship model for internal auditor certification, risk assessment, and the role of senior management on the effectiveness of cybersecurity in internal auditors that did not exist in previous studies. A cybersecurity checklist is very important since investing in cybersecurity can be a complex process. An organization must first identify a vulnerable asset, determine how vulnerable it is, and allocate sufficient budget to improve its security. The company's cybersecurity program includes procedures to identify and assess cybersecurity threat risks, anticipate data and security breaches, plan and implement asset recovery plans that are lost or lost.

References

AlDaajeh, S., Saleous, H., Alrabaee, S., Barka, E., Breitinger, F., & Choo, K. K. R. (2022). The role of national cybersecurity strategies on the improvement of cybersecurity education. *Computers & Security, 119*, 102754.

Arpaci, I., & Aslan, O. (2023). Development of a scale to measure cybercrime-awareness on social media. *Journal of Computer Information Systems, 63*(3), 695-705.

Chaudhary, S., Gkioulos, V., & Katsikas, S. (2022). Developing metrics to assess the effectiveness of cybersecurity awareness program. *Journal of Cybersecurity, 8*(1), tyac006.

Creemers, R. (2023). Cybersecurity Law and Regulation in China: Securing the Smart State. *China Law and Society Review, 6*(2), 111-145.

Eboibi, F. E., & Ogorugba, O. M. (2023). Cybercrime Regulation and Nigerian Youths Increasing Involvement in Internet Fraud: Attacking the Roots Rather than the Symptoms. *Journal of Legal Ethical & Regular Isses, 26*, 1.

Hair, J. F., Sarstedt, M., Ringle, C. M., & Mena, J. A. (2012). An assessment of the use of partial least squares structural equation modeling in marketing research. *Journal of the academy of marketing science*, *40*, 414-433.

Kemp, S. (2023). Exploring public cybercrime prevention campaigns and victimization of businesses: A Bayesian model averaging approach. *Computers & Security, 127*, 103089.

Kurniawan, Y., & Mulyawan, A. N. (2023). The Role of External Auditors in Improving Cybersecurity of the Companies through Internal Control in Financial Reporting. *Journal of System and Management Sciences, 13*(1), 485-510.

Khan, N. F., Ikram, N., Murtaza, H., & Javed, M. (2023). Evaluating protection motivation based cybersecurity awareness training on Kirkpatrick's Model. *Computers & Security, 125*, 103049.

Kumar, G., Pandey, S. K., Varshney, N., Kumar, A., Kumar, M., & Singh, K. U. (2023, April). Cybersecurity Education: Understanding the knowledge gaps based on cybersecurity policy, challenge, and knowledge. In 2023 IEEE 12th International Conference on Communication Systems and Network Technologies (CSNT) (pp. 735-741). IEEE.

Li, Y., Goel, S., & Williams, K. J. (2023). Exploring Antecedents of Professional Skepticism on Accounting Students' Performance in Cybersecurity. *Journal of Emerging Technologies in Accounting, 20*(1), 147-168.

Lim, A., Brewer, N., & Young, R. L. (2023). Revisiting the relationship between cybercrime, autistic traits, and autism. *Journal of Autism and Developmental Disorders, 53*(4), 1319-1330.

Masoud, N., & Al-Utaibi, G. (2022). The determinants of cybersecurity risk disclosure in firms' financial reporting: Empirical evidence. *Research in Economics, 76*(2), 131-140.

Mijwil, M., & Aljanabi, M. (2023). Towards artificial intelligence-based cybersecurity: the practices and ChatGPT generated ways to combat cybercrime. *Iraqi Journal For Computer Science and Mathematics, 4*(1), 65-70.

Nobles, C. (2022). Stress, burnout, and security fatigue in cybersecurity: A human factors problem. *HOLISTICA–Journal of Business and Public Administration, 13*(1), 49-72.

Nwankpa, J. K., & Datta, P. M. (2023). Remote vigilance: The roles of cyber awareness and cybersecurity policies among remote workers. *Computers & Security, 130*, 103266.

Nyre-Yu, M., Morris, E., Moss, B. C., Smutz, C., & Smith, M. (2022, April). Explainable AI in Cybersecurity Operations: Lessons Learned from xAI Tool Deployment. In Proceedings of the Usable Security and Privacy (USEC) Symposium, San Diego, CA, USA (Vol. 28).

Shillair, R., Esteve-González, P., Dutton, W. H., Creese, S., Nagyfejeo, E., & von Solms, B. (2022). Cybersecurity education, awareness raising, and training initiatives: National level evidence-based results, challenges, and promise. *Computers & Security, 119*, 102756.

Steinmetz, K. F., Schaefer, B. P., Brewer, C. G., & Kurtz, D. L. (2023). The Role of Computer Technologies in Structuring Evidence Gathering in Cybercrime Investigations: A Qualitative Analysis. *Criminal Justice Review,* 07340168231161091.

Oumaima, C., Abdeslam, R., Yassine, S., & Abderrazek, F. (2022). Experimental study on the effectiveness of machine learning methods in web intrusion detection. In Advances in Information, Communication and Cybersecurity: Proceedings of ICI2C'21 (pp. 486-494). Springer International Publishing.

Parker, S., Wu, Z., & Christofides, P. D. (2023). Cybersecurity in process control, operations, and supply chain. *Computers & Chemical Engineering*, 108169.

Purwanto, A., Purba, J.T., Bernarto, I., Sijabat, R. (2023).Investigating the role digital transformation and human resource management on the performance of the universities. *International Journal of Data and Network Science, 7*(4). DOI: 10.5267/j.ijdns.2023.6.01128.

Pratiwi, H. A., & Wulandari, L. (2021). Evaluasi Tingkat Kesiapan Keamanan Informasi Menggunakan Indeks Keamanan Informasi (Indeks KAMI) Versi 4.0 pada Dinas Komunikasi dan Informatika Kota Bogor. *Journal of Industrial Engineering & Management Research, 2*(5), 146 - 163. https://doi.org/10.7777/jiemar.v2i5.196

Sam, M. F. M., Ismail, A. F. M. F., Bakar, K. A., Ahamat, A., & Qureshi, M. I. (2022). The Effectiveness of IoT Based Wearable Devices and Potential Cybersecurity Risks: A Systematic Literature Review from the Last Decade. *International journal of online and biomedical engineering, 18*(9), 56-73.

Slapničar, S., Vuko, T., Čular, M., & Drašček, M. (2022). Effectiveness of cybersecurity audit. *International Journal of Accounting Information Systems, 44,* 100548.

Selimoglu, S. K., & Saldi, M. H. (2023). Blockchain Technology for Internal Audit in Cybersecurity Governance of Banking Sector in Turkey: A SWOT Analysis. *In Contemporary Studies of Risks in Emerging Technology, Part B* (pp. 23-55). Emerald Publishing Limited.

Utomo, H. J. N., Irwantoro, I., Wasesa, S., Purwati, T., Sembiring, R., & Purwanto, A. (2023). Investigating The Role of Innovative Work Behavior, Organizational Trust, Perceived Organizational Support: An Empirical Study on SMEs Performance. *Journal of Law and Sustainable Development, 11*(2), e417. https://doi.org/10.55908/sdgs.v11i2.417

Valiyev, A., oglu Rustamov, F. V., Huseynova, R. A., Orujova, M. S., & Musayeva, S. N. (2022). The digitalization effectiveness as an innovative factor development of the agriculture in Azerbaijan. *Journal of Eastern European and Central Asian Research (JEECAR), 9*(2), 194-205.

Victory, C. O., Promise, E., & Mike, C. N. (2022). Impact of Cyber-Security on Fraud Prevention in Nigerian Commercial Banks. *Jurnal Akuntansi, Keuangan, dan Manajemen, 4*(1), 15-27.

Yusif, S., & Hafeez-Baig, A. (2023). Cybersecurity Policy Compliance in Higher Education: A Theoretical Framework. *Journal of Applied Security Research, 18*(2), 267-288.

Wissink, I. B., Standaert, J. C., Stams, G. J. J., Asscher, J. J., & Assink, M. (2023). Risk factors for juvenile cybercrime: A meta-analytic review. *Aggression and Violent Behavior*, 101836.

Wu, L., Peng, Q., & Lembke, M. (2023). Research Trends in Cybercrime and Cybersecurity: A Review Based on Web of Science Core Collection Database. *International Journal of Cybersecurity Intelligence & Cybercrime, 6*(1), 5-28.

Wylde, V., Rawindaran, N., Lawrence, J., Balasubramanian, R., Prakash, E., Jayal, A., ... & Platts, J. (2022). Cybersecurity, data privacy and blockchain: a review. *SN Computer Science, 3*(2), 127.