A proposed Framework for Studying the Impact of Cybersecurity on Accounting Information to Increase Trust in The Financial Reports in the Context of Industry 4.0: An Event, Impact and Response Approach

Asmaa AbdElmonem Serag

Lecturer of Accounting

Faculty of Commerce

Tanta University

Asmaa_serag@commerce.tanta.edu.eg

Mona Mohamed Ali Daoud

Lecturer of Accounting

High Institute of Management

Al mahalla Alkobra

Monadaoud1980@gmail.com

Abstract

Industry technologies include Big data, internet of things, system integration, cloud computing , Rebotics , automation augment and virtual reality. Cybersecurity help guarantee that these technologies and essential information they contain remain sale and protected. As Interconnection and the usage of electronic data gathering, storage, and transfer become more prevalent, with significant industry adoption, and that increasing the number of business being targeted for cybertheft, damage or disruption. Cybersecurity means all steps to safeguard business against illegal electronic data usage. Manufacturers Can remain secure and prosperous by protecting all hardware, software, and information from internal and external threats. These breaches have implications for business enterprises as they may result in lower performance and market value, increased operational risks, lost information and significant employee time spent ensuring compliance with appropriate privacy and confidentially regulations.

The proposed framework depends on an event, impact and response approach to identify directions for accounting and auditing. This framework aims to examine how cybersecurity impacts cybersecurity events or threats, and how these events impact organisations and responses by various parties to different events. Based on COSO Enterprise Risk Management Framework, organisations need to identify the impact of cybersecurity threats, then follow up by developing responses to the related risks by using cause and effect relationship between risks and responses.

Thus, this research aims to develop a framework for linking existing cybersecurity research to accounting. This framework gives look forward information and insights to researchers and practionners. Accountants should involved in identifying and measuring the costs of cybersecurity events; tracking the impact of these events on the organcisations; ensuring the organisations to disclose cybersecurity threats appropriately to investors and finally auditors should often adjust their risk assessment and audit procedures due to the presence of cybersecurity events.

The proposed framework highlights how practitioners can better assess cybersecurity threats, understand their impact, and develop responses strategies. Furthermore, the researches about cybersecurity need to extended beyond AIS to other areas. Such as financial accounting, managerial accounting and auditing.

Keywords: cybersecurity; cyberthreats; cybersecurity Disclosures; Cybersecurity Risk Management Program; Industry 4.0.

1/ Introduction :

The growing dependence of both public and private firms on information technologies and networks for their financial management systems increases their vulnerability to cyber threats. In addition, the economy has become more knowledge-based; therefore, protecting information assets has become a top agenda item for accountants and managers (Gordon et al., 2010). Cybersecurity has thus increased, becoming one of the most significant risk management challenges facing every type of organization.

In addition to new threats, the cost of cyber related crimes has increased (Accenture,2019).With the increasing number of threats and reported vulnerabilities, organizations are challenged to ensure confidentiality, integrity, and availability of the data (A ICPA, 2017), to detect the attacks and respond to / recover from data breaches, every organization should implement a cybersecurity program or a cybersecurity strategy. This also applies to countries. Moreover, many countries frequently identify the state agencies in charge of setting minimum standards and responding to cyber incidents (World Bank, 2018).

These breaches have implications for business enterprises as they may result in lower performance and market value, increased operational risks, lost information, and significant employee time spent ensuring compliance with appropriate privacy and confidentiality regulations (Ponemon, 2018). So, we argue that a

more systematic framework for linking cybersecurity to accounting is needed. Accountants are involved in identifying and measuring the costs of cybersecurity events and tracking the impact of these events on the organizations, ensuring organizations appropriately disclose cybersecurity events to investors. Auditors often adjust their risk assessment and audit procedures due to the presence of cybersecurity events.

This paper develops a Framework based on the Event, Impact, Response approach to identify key directions for accounting practitioners and researchers to improve cybersecurity risk management process and to increase the trust and the transparency of financial reports in the context of Industry 4.0 . For practitioners, while cybersecurity events are often difficult to identify and assess, conceptual frameworks from management information systems and computer science can help organizations better detect potential cybersecurity events. Further, our understanding of the impact of cybersecurity on operational, reputational, compliance and litigation risks is still quite limited. Joint work between practitioners and researchers may help more understanding and preparing for its impact.

2/ Literature Review and Problem Statement:

The increasing use of digital technologies among companies has emphasized the importance and role of cybersecurity as a new risk management dimension. Furthermore, firms hit by cyber-attacks tend to suffer long-lasting economic and reputational losses. Recent studies (Gordon et al., 2015b ; IIA, 2018; Islam et al., 2018) suggest that over just a few years, cybersecurity has grown into one of the most significant risk challenges facing every type of organizations, because cybersecurity breach could shut down an entire critical infrastructure industry and threaten a nation’s entire economy and national defense.

And based on its importance , literatures contain several studies that represent a variety of cybersecurity issues using several research methods and theories. Figure (1) shows the research streams and factors related to cybersecurity (Haapamäki & Sihvonen, 2019) :

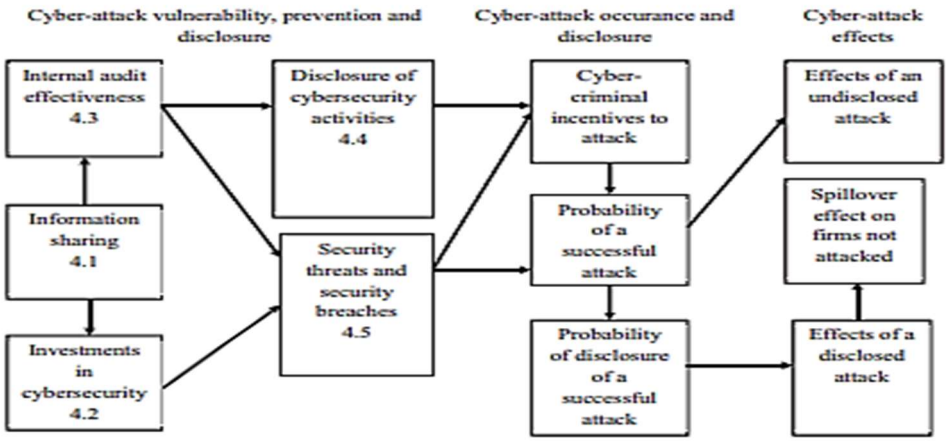

Figure 1: Research streams and factors related to cybersecurity
Source : (Haapamäki & Sihvonen, 2019)

The first research stream examines information sharing and its role in cybersecurity. The prior literature has suggested that information sharing in cybersecurity has become extremely important for accounting and public policy. For instance, (Gordon et al., 2015a) examined information sharing in relation to computer system security. Their findings indicated that sharing information about threats and breaches of computer security lowers the overall costs of achieving any particular level of cybersecurity. companies and society could benefit from sharing information concerning security breaches. The study added that sharing information is a key element required to improve cybersecurity , because having information on threats and on actual incidents experienced by others can help an organization better understand the risks faced and determine what preventive procedures should be implemented . Furthermore, the study suggested that the benefit gained from information sharing could

provide a vital incentive to overcome firms' unwillingness to share their private information actively.

The second research stream identified concentrates on cybersecurity investments. Given the significance of cybersecurity to organizations, a fundamental economics-based question has been brought up regularly in prior studies: How much should be invested in cybersecurity related activities? (Gordon et al., 2016) presented a model which it is known as the Gordon–Loeb Model. information security is a growing spending priority for most companies around the world, which prompted them to create an economic model that determines the optimal amount to invest in information security. The Gordon–Loeb Model is applicable to investments related to various information-security goals, for instance protecting the confidentiality, availability and integrity of information.

Hence, their findings indicated that the optimal amount to spend on protecting information sets does not always increase with the level of vulnerability of such information. So, the amount that a firm should spend on protecting information sets should generally be only a small fraction of the expected loss, and accordingly, the findings showed that "managers allocating an information-security budget should normally focus on information that falls into the midrange of vulnerability to security breaches. Since, extremely vulnerable information sets may be inordinately expensive to protect, a firm may be better off concentrating its efforts on information sets with midrange vulnerabilities.

Other papers examine how managers react to data security breaches, (Xu et al., 2019) explore whether managers are more likely to engage in earnings management following detection of data security breaches. Their findings suggest that firms are more likely to engage in real earnings management when the breach is related to financial information, the disclosure of the breach is delayed . (Banker and Feng, 2019) also examine how managers

respond to detected data security breaches by examining the association between detected data security breaches and chief information officer (CIO) turnover. The authors argue that security breaches reflect the CIO's information technology (IT) performance. When the CIOs fail to meet this performance expectation (i.e., a breach occurs), the likelihood of turnover will increase. Their findings demonstrate that the breach increase CIO turnover likelihood by 72 percent.

The next study examines the economic impact of privacy breaches. Specifically, (Richardson et al., 2019) explore whether data privacy breaches impact organizations' abnormal returns, future accounting measures of performance, insider sales, and reporting of SOX Section 404 internal control material weaknesses. Results indicate that, on average, the economic consequences of privacy breaches on firms' cumulative abnormal returns, future accounting measures of performance such as sale growth return on sales and operating expense, higher audit and other fees, and future SOX 404 reports of material internal control weaknesses are generally very small.

In addition, (Frank et al., 2019) examine whether a prior cyberattack influences the efficacy of cybersecurity risk management reporting and independent assurance. The authors design an experiment to capture how disclosures proposed by AICPA may influence nonprofessional investors' perceptions. The study concluded that issuing a management's report without assurance is more effective when a company has not disclosed a prior cyberattack. Further, issuing an independent cybersecurity assurance report may increase a company's ability to attract investments. Finally, (Cheng & Walton, 2019) explore whether the timing and source of data breaches impact investors' reactions to the data breaches. By using an experimental setting, the authors demonstrate that investors are less likely to invest in a company if the breach is announced by the company itself, as compared to an

outside source. However, timeliness does not seem to be a major factor in whether investors will invest in a company with a data breach.

On the other hand, many studies have researched the problems of accounting data security in conditions of active cyber threats at micro and macro levels. For instance, the study of (Janvrin & wang , 2019) formulated a comprehensive definition of cybersecurity from the accounting point of view. It defines cybersecurity as "the security from internal and external threats of the enterprise's vital interests, human and intellectual capital, trade secrets, proprietary technologies, profits, added and market value, information created by the accounting system and provided for by special legal, economic, organizational, informational and technical measures". It also determined the fundamental principles of measures for accounting data cybersecurity, namely: software support, protection of confidential information, personal responsibility, confidentiality, comprehensiveness, and control over access to accounting data. Most studies attributed the need for cybersecurity at micro and macro levels to the increasing development of communication technologies , the digitalization of economic activities and business processes and the emergence of cyberspace, there have been more criminal acts aimed to illegal financial gain.

Framework of operational responsibilities of accounting personnel in the event of cyberattacks is an important direction of research that establishes the role of accounting in ensuring security. (Haapamäki & Sihvonen, 2019) have developed instructions for avoiding, overcoming and minimizing the effects of the cyber impact on economic systems of the enterprise. Similarly, the study of (accenture, 2019) has outlined the measures aimed at minimizing internal, accidental and external threats to cybersecurity. It defined cybersecurity of the enterprise as " a set of actions carried out by accounting personnel with the purpose of archiving data, maintaining the professionalism level of

accounting specialists, building an effective communication system between the enterprise and the stakeholders, creating optimal work conditions for accountants" .

It is recommended to associate the cybersecurity functions with the accounting system of the enterprise in order to optimize the information and security processes. Ensuring cybersecurity involves not only protecting accounting data, but also making accounting the basis for ensuring cybersecurity of enterprises and the integrator of methodological and organizational actions aimed at maintaining information and economic security of economic entities, branches and sectors of the economy.

Previous studies (Deloitte, 2016a; 2016b) concentrated on responses to publicly identified breaches even though organizations generally spend more resources on addressing threats to prevent incidents and breaches than on responding to these publicly available breaches. Our analysis finds that most existing accounting-related cybersecurity research examines how investors react to either organization-provided or externally provided cybersecurity related disclosures. More research is needed exploring how organizations detect cybersecurity events and how organizations assess and manage cybersecurity threats. Second, current accounting-related research investigates the impact of cybersecurity on operational performance and business value. Additional accounting-related work is needed to examine how cybersecurity impacts operational, reputational, compliance and litigation risks. Third, existing response literature addresses management actions regarding employee training and cybersecurity strategy, investor responses (i.e., market reaction), and auditor responses. Research examining how management reacts to or monitors public perceptions, invests in additional IT infrastructure, and / or purchases cybersecurity insurance, and whether interested parties initiate lawsuits is still very limited.

Finally, the impact of cybersecurity issues extends beyond the information systems community and we encourage financial accounting, auditing, and managerial accounting researchers to contribute to this important topic by providing a discussion of current theories used in this research. Existing studies published in information systems journals use a wide variety of theories from management, psychology, and criminology. Accounting researchers may bring new thoughts to cybersecurity research by building different theoretical backgrounds.

So, this research is important for several reasons. First, cybersecurity risk management is an interdisciplinary area that ranges from strategies to technical solutions. It impacts business operations and may affect all firm stakeholders. So, understanding, assessing, monitoring, and responding to cybersecurity threats become a critical research topic for accounting researchers. Second, regulators are concerned about organizations' ability to respond to cybersecurity incidents and breaches. The SEC's recent cybersecurity guidance (SEC, 2018) and the AICPA's efforts to develop its Cybersecurity Risk Management Reporting Framework (A ICPAs, 2018a). Specifically, the SEC states "it is critical that public companies take all required actions to inform investors about material cybersecurity risks and incidents in a timely fashion" . This Event, Impact, Response Framework assists practitioners and researchers in identifying the actions (or responses) needed. Third, the proposed framework encourages broader research as it expands cybersecurity interest beyond the accounting information systems research community to financial accounting, managerial accounting, and auditing. For example, financial accounting researchers may provide insights regarding cybersecurity disclosures while managerial accounting researchers may examine incentives and monitoring mechanisms for managing cybersecurity threats. Audit researchers may examine how internal and external auditors evaluate clients' cybersecurity risks as they plan and execute their audits.

3/ Research Objectives:

This research aims to link the cybersecurity threats and accounting information by developing a framework that depends on an event, impact and response approach.

This proposed framework helps in improving the classification of accounting information users related to cybersecurity threats.

4/ Research Methodology:

This paper aims to build a proposed framework to asset accounting as an innovative multilevel mechanism of ensuring the interaction of cyber threats and accounting information four levels of information interaction between cybersecurity of enterprises and information are identified. First; methodological level, showed the impact of cyber threats on the principles and functions of accounting and economic level, second; impact on accounting information quality, third; the methodological level; impact on accounting types and accounting items. Fourth; the communication with stakeholders. The "positivistic methodology" is needed to describe and predict the relationship between accounting information and cybersecurity threats.

5/ Cybersecurity Conceptual Framework :

Cybersecurity is an analogous term for information security. According to (SEC, 2018) cybersecurity can be defined as " the activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification, or exploitation". However, cybersecurity is not necessarily only the protection of cyberspace itself but also the protection of those who function in cyberspace and any of their assets that can be reached via cyberspace. Cybersecurity comprises technologies, processes and controls that are designed to protect systems, networks and data from cyberattacks.

Effective cybersecurity reduces the risk of cyber-attacks and protects societies, organizations and individuals from the unauthorized exploitation of systems, networks and technologies. Cybersecurity is an umbrella concept that encompasses information security and information assurance (Amir et al., 2018; Li et al., 2018). Thus, cybersecurity involves the protection of information that is assessed and transmitted via any computer network

Cybersecurity uses technology and processes to prevent cyber threats on systems, networks, programs, devices, and data. Its goal is to limit the risk of cyber threats and secure systems, networks, and technology from unauthorised use. The necessity of cybersecurity continues to expand as the number of people, devices, and programs in the modern company grow, along with the rising deluge of data, most of which is sensitive or confidential. The problem is exacerbated by the increasing number and sophistication of cyber attackers and attack strategies (Muravskyi,2022). It is challenging to stay up with new technology, security trends, and threat intelligence. It has required safeguarding data and other assets against cyberthreats, which can take numerous forms. Malware, ransomware, phishing, distributed denial-of-service (DDoS), advanced persistent threats (APTs), man-in-the-middle (MitM), and other cyber threats are a few examples.

According to (Gordon et al.,2010), the objectives of cybersecurity can be divided into three broad categories. First, cybersecurity protects the confidentiality of private information; second, it ensures that authorized users can access information on a timely basis and third, cybersecurity protects the accuracy, reliability and validity of information.

The American Institute of Certified Public Accountants (AICPA, 2018a) stated that “Cybersecurity is one of the top issues on the minds of management and boards in nearly every company in the

world, large and small, public and private." Therefore, it is extremely important that every organization at least consider a cybersecurity risk management program. In addition, certain organizations and their stakeholders need timely, useful information about organizations' cybersecurity risk management efforts. Therefore, the (AICPA, 2018b) highlighted that cybersecurity is not just an information technology (IT) problem; it is an enterprise risk management problem that requires a global solution. The AICPA also emphasized the importance of the entity-level cybersecurity reporting framework. It explicitly stated that the goal of the reporting framework is to provide a means by which organizations can communicate useful information regarding their cybersecurity risk management programs to stakeholders.

Hence, the reporting framework is used to perform an examination-level attestation engagement. The framework is a key component of a new System and Organization Control (SOC) for cybersecurity engagement. The cybersecurity report includes three key sets of information : management's description; management's assertion and practitioner's opinion.

Briefly, the (AICPA ,2018b) emphasized that its cybersecurity risk management reporting framework is a crucial first step toward enabling a consistent, market-based, business-based solution for companies to communicate successfully with key stakeholders on how they are managing cybersecurity risk. In addition, the Securities and Exchange Commission (SEC, 2018) argued that it is essential that : Public companies take all required actions to inform investors about material cybersecurity risks and incidents in a timely fashion, including those companies that are subject to material cybersecurity risks but may not yet have been the target of a cyber-attack.

6/ The Need for Cybersecurity for Industry 4.0:

Industry 4.0 refers to the interconnection of Cyber-Physical Systems which connects the physical and digital worlds by collecting digital data from physical objects/processes and using this data to drive automation and optimisation. Digital technologies used in this revolution gather and handle massive volumes of high-velocity streams while automating field operations and supply chain activities. Cybersecurity is a complicated process that helps sort out various hacking issues of Industry 4.0. The rise of Industry 4.0 technologies is changing how machines and associated information are obtained to evaluate the data contained within them. Cybersecurity results in high-end products, with faster and better goods manufactured at a lower cost.

Therefore, Industry 4.0 technologies are expected to drive evolution in the traditional linear supply chain structure by introducing intelligent, connected platforms and devices throughout the ecosystem, resulting in a digital supply network. Cybersecurity can capture data from points throughout the value chain and also reduces the chances of hacking. So, there is a need to study the significant capabilities of cybersecurity in Industry 4.0. Consequently, there may be improved management and flow of materials and commodities, more efficient use of resources, and supply that better suit the demands of customers (Industrial Robot,2021).

Also, data analytics are used in cybersecurity to gather knowledge that drives process improvements. These operations need advanced analytics, such as deep learning and artificial intelligence. By using this technology, supply chains become more dynamic, adaptable, interconnected, and performance-demanding with the introduction of intelligent manufacturing. Because supply chains are interconnected, current and emerging security threats might have a broader impact. Cybersecurity is critical to keep the corporate networks up to date to minimise possible security risks.

This technology drives towards Industry 4.0 by making operations quicker and easier. Manufacturing cybersecurity defences are essential safeguards.

In fact, Industry 4.0 relies heavily on the seamless integration of the supply chain into the production process. Suppliers, manufacturers, and end customers work together with quick information sharing in the ideal world. These types of collaborations reduce production inefficiencies, procurement cost savings, automated decision making, consistent data and communication between manufacturers and suppliers, and product agility or customization

Figure (2) shows some of the emerging cyber security technologies. Data may be protected with Artificial Intelligence

(AI) technology against increasingly sophisticated and harmful cyber-attacks. Although AI is not yet conscious, it is expected to have a future in predicting and mitigating cyber-attacks . User-behavioural analytics aids in the detection of possible and real-time cyber threats by identifying trends in a system's and network's activity. An unusual rise in data transfer from a specific user device, for example, could suggest a potential cyber security risk. While behavioural analytics is commonly utilised in networks, now it is increasingly applied in systems and consumer devices. Thus, this system employs big data analytics to detect any suspicious behaviour.

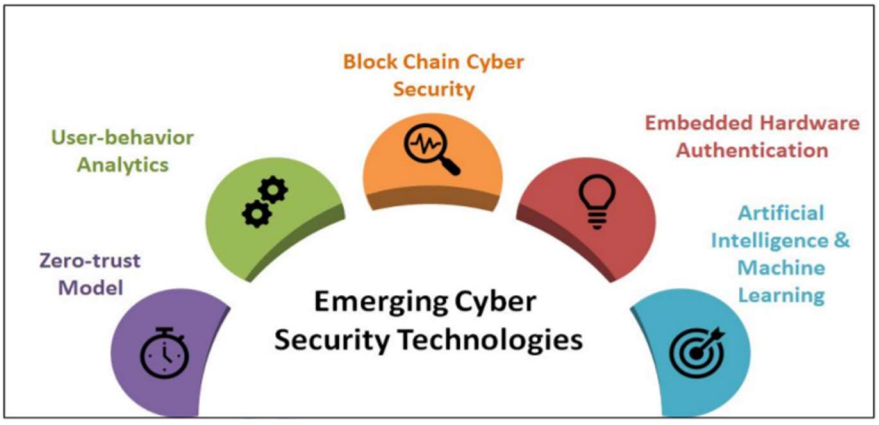

Figure 2: Emerging Cyber Security technologies

Source : (Industrial Robot,2021).

So, Cybersecurity is required for Industry 4.0 to function, not just in technological terms but also in value chain operations. Blockchain and Artificial intelligence technology are helpful emerging technologies for Cyber security. The tenet of Industry 4.0 is that a manufacturing company will achieve higher efficiency, productivity, and autonomous operation of production processes by ensuring that machines/plant equipment, logistics systems, work-in-progress components, and other elements communicate directly with each other achieve collaboration

Cybersecurity is vital for small and medium-sized manufacturing firms since employees frequently conflate a computer attack with a breakdown production system. Even though the amount and importance of data taken are typically less when compared to those of major multinational organisations, small and medium-sized businesses are the most enticing to hackers. The business has become an increasingly rewarding field for potential hackers. The increased usage of electronics and computers resulted in lower costs, computer downsizing and durability, and a significant rise in computing and processing capacity. The convergence of digital and communication technologies began. The combination of digital and industrial technologies is poised to change production and contribute to the realization of the Industry 4.0 goal.

Also, Figure 3 illustrates the several features and progressive steps in realising cybersecurity in the industry 4.0 domain., and from the basics of industry 4.0 and cybersecurity, this has been become a common trend and needs to explore the security of enabled systems and other allied issues. The major complex and multiple critical domains are; network security, incident management, prevention against malware, secure configurations, control systems, security, etc. This further ensures a secure and safe practice throughout the industry 4.0 domain .

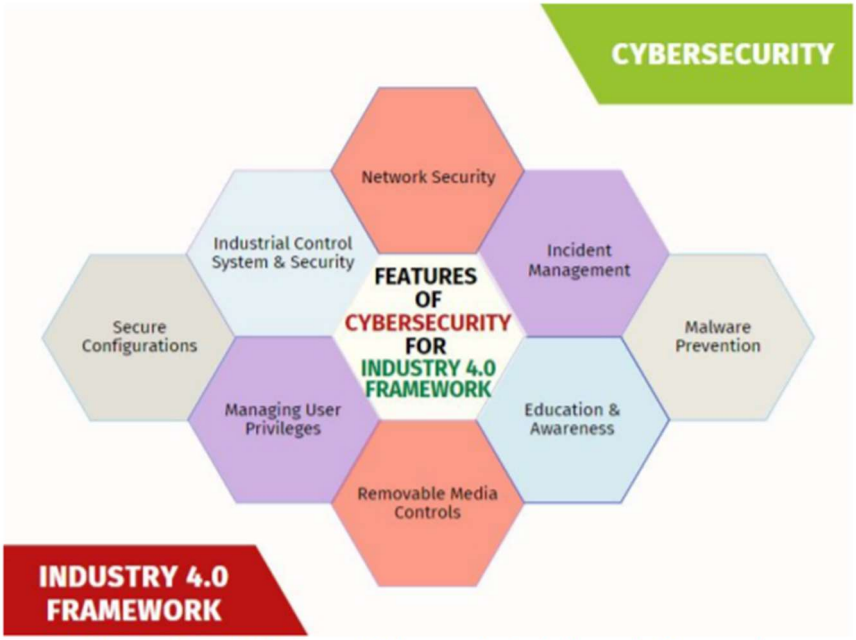

Figure 3: Potential Features of Cybersecurity for Industry 4.0 Framework

Source : (Industrial Robot,2021).

Thus, businesses must do regular software patching and vulnerability checks to avoid hacker operations. The progress of cyber security technology in risk containerisation, threat segmentation, network zoning, and profiling has resulted in their widespread use in enhancing a company's cyber posture. Organisations also use language recognition and behavioral pattern mapping to improve risk management approaches and policies. Through the use of cyber security, any device, application, or program with direct, remote, or even indirect access to an organization’s systems must be closely monitored . Mapping out the whole overlay of connection points enables security teams to assess vulnerabilities and strengthen restrictions. Real-time connection monitoring, visualising and sending alarms for any aberrant, unverified activity to minimise security breaches are critical in minimising Industry 4.0 threats.

Additionally, Cloud architectures and ubiquitous computing, big data, and virtualisation are developing as technologies with a limited presence in the Industry. Emerging systems of cyber-physical production, traditional operations, and support in information technology are beginning for real and virtual worlds. Industry 4.0 is characterised as a set of distinguishing traits aimed at integrating other intelligent infrastructures such as mobile or logistic infrastructures and intelligent buildings and accelerating technological progress. Cybersecurity provides a quick reaction to dynamic changes, like changes in demand, stock, or probable mistakes. The emphasis is on improving resource efficiency, notably in materials, energy, and human resources. New networks operate in real-time, providing more transparency and more flexible and resilient service .

7/ Theoretical Foundation of the Relationship between Accounting and Cybersecurity of the Enterprise :

The accounting system should be a platform for organising cybersecurity because the accounting system is the main producer of economic information, therefore the accounting processes should be prioritised in cybersecurity matters. Much of the accounting information - except the financial statements - contains trade secrets as it is used for the operational, tactical and strategic planning by the management. On the other hand, most of the latest hacker attacks and fraudulent schemes have been conducted through accounting and management software, which explains the importance of protecting the accounting system .

Organization of cybersecurity using the accounting system as the basis entails the expansion of the operational responsibilities of the accounting and internal control departments or an addition of the cybersecurity specialist post to the enterprise's staff. The feasibility of organisational transformations must be justified by their economic effectiveness, regardless of the size and scope of the business. Also, modern accountants should be multi-qualified

professionals who combine economic, technical and legal knowledge and can perform cybersecurity functions at the enterprise. the regulatory framework for the accounting system defines most information processes at the enterprise and some regulations may contain guidelines on ensuring cybersecurity.

According to the (SEC, 2018) report, 80% of cybercrime targeted small businesses through mail services, social networks, and cloud services. The main reason cyberattacks center on small-scale business is the lack of specialists and departments ensuring cyber security. Therefore, the likelihood that these cyberattacks will be successful on such businesses is higher. Specialists on accounting or control can successfully perform the cybersecurity functions at small enterprises. Therefore, cybersecurity specialists should divided into 3 groups :

(1) specialists on information security (accounting staff) .
(2) control department specialists (testing information systems on vulnerability to breaches, cybersecurity analysts, internal controllers, security auditors, inspectors on confidential information security) .
(3) technical support staff (system administrators, computer network administrators, programmers of specialised systems and web technology).

Cybersecurity specialists must have a comprehensive understanding of information processes at the enterprise, the information and technological infrastructure, the interactions with external stakeholders and contractors. It would be prudent to instruct the employees of the first category in the course of the accounting specialists' professional training. The second group may consist of the accounting personnel who have practical experience in the field of cyber security and have acquired additional multidisciplinary skills and knowledge. Only the employees of the third group would be trained in technological field that does not envision obtaining in-depth knowledge of the economic disciplines, including accounting, analysis and control.

Thus, the operational responsibilities of accounting specialists of the first and the second group include: identifying vulnerabilities of the information systems and modelling the likely scenarios of cyber threats and risks related to them; verifying the reliability of security system operation, developing security measures in the event of unforeseen circumstances; classifying accounting information as restricted (commercial and trade secrets, other confidential information); developing regulations, policies and procedures in the framework of accounting information security; implementing developed security measures, testing the system in order to evaluate its effectiveness, and making adjustments as needed; assigning the necessary security details to the accounting computer system users; teaching the rules of continuous information processing to information system users; ensuring that information system users and company staff adhere to the rules of working with accounting information .

Also, it is important to regulate the operational responsibilities of cybersecurity in the employee handbook of accounting specialists and to define liability for violations of enterprise cybersecurity. Such responsibility may be not only administrative but also criminal, as the actions of accounting specialists may harm both the cyber security of a single enterprise and the national security of an entire sector of the economy. Additionally it is recommended to recognize the responsibility for effective cybersecurity of the enterprise in the ethics code of professional accountant.

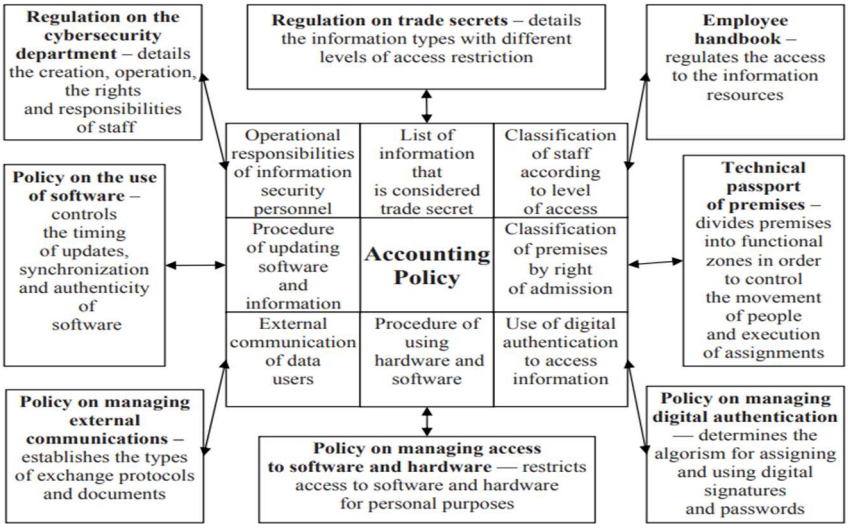

Fig. **Security protocols documented in the enterprise accounting policy and internal regulations**

As shown in figure No.4, it is proposed to document several security protocols in the accounting policy and certain internal regulations of the enterprise. These include: the list of information that constitutes trade secret; the procedure of updating software and the methodology of cloud synchronization of information; external communications done by the data users; procedures of using software and hardware; algorism of assigning and using digital authentication to access information; classification of premises by right of admission and organisation of enterprise sites; hierarchal classification of employees by level of access to information resources of the enterprise. Combining all regulations on cybersecurity in the accounting policy will ensure that the enterprise operation goals, its accounting, analytical, control and management systems correspond to effective cyber security.

8/ A Proposed Framework for Studying the Impact of Cybersecurity on Accounting Information Based on An Event, Impact and Response Approach :

This framework aims to examine how cybersecurity impacts accounting information , the framework concentrates on cybersecurity events or threats, how these events impact organizations, and responses by various parties to these events. Event, Impact, Response approach depends the COSO Enterprise Risk Management Framework, which notes that organizations need to identify the impact of threats, in this case cybersecurity

threats, and to follow up by developing responses to the related risks. (COSO 2017; Janvrin & wang , 2021).

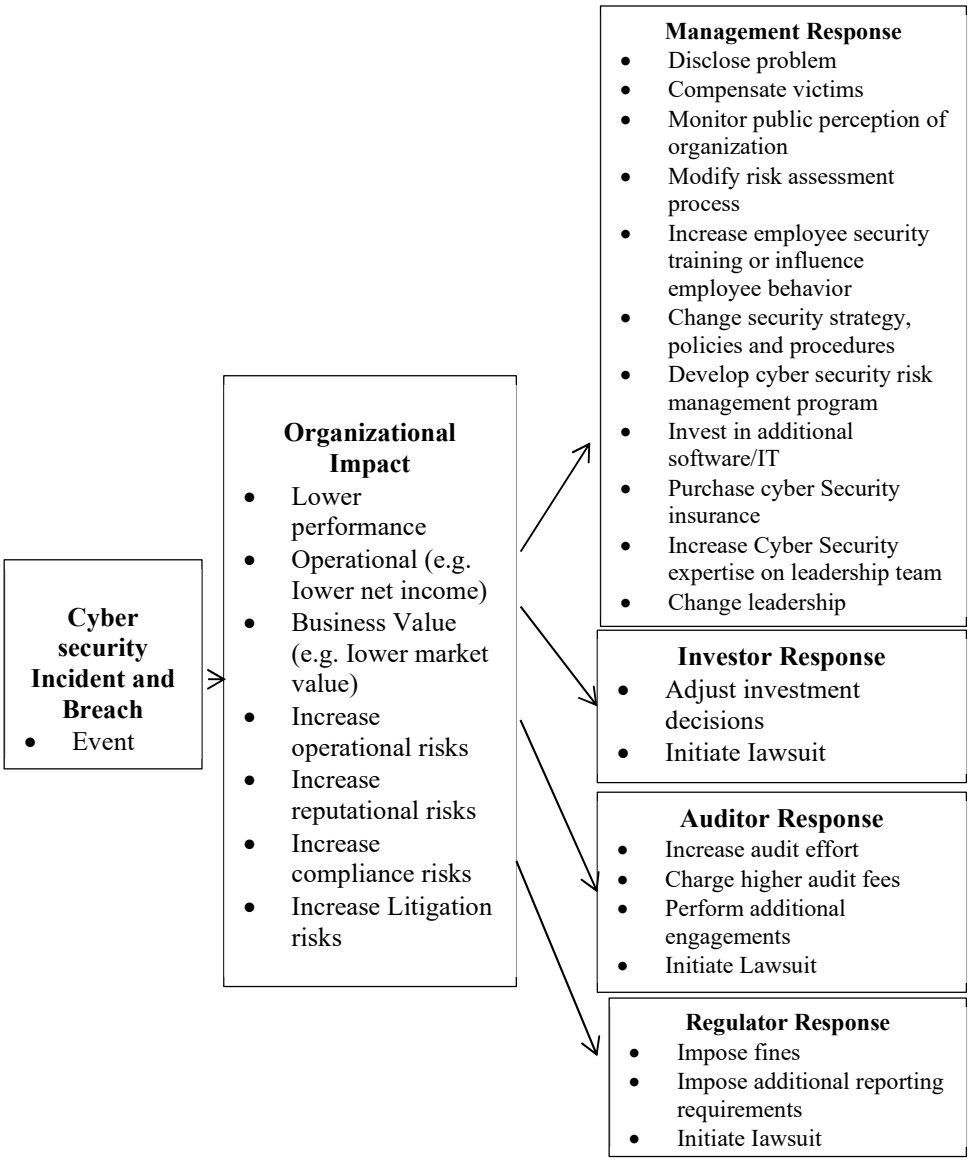

FIGURE 5: Effect of Cyber security on Accounting Information: Event, Impact, and Response Framework

8/1 Cybersecurity-Related Events:

Event, Impact, Response Framework begins with cybersecurity-related events including threats, incidents, and breaches. Once management acknowledges cybersecurity threats exist, they may respond by developing a risk assessment plan. If a threat agent exploits vulnerability, it becomes an incident or breach. Cybersecurity incidents and breaches can occur at any time. Importantly, cybersecurity incidents and breaches must be detected before organizations can examine their impact and how various interested parties can respond. Further, incidents and breaches may not be disclosed immediately upon detection due to time needed for organizations to identify their impact.

(Boritz and No, 2005) discussed security threats and the limitations of security technologies, and the security requirements to ensure reliable, trustful financial reporting services. The study also explained several proposed security standards and suggested the Web Services Security Architecture as a suitable security mechanism for financial reporting services. Similarly, (Abu-Musa, 2006) investigated the perceived security threats to computerized accounting information systems in the Egyptian banking industry and emphasized that advanced technology has created significant risks related to ensuring the security and integrity of computerized accounting information systems. However, the findings of the study revealed that the most significant security threats are the accidental entry of bad data by employees, the accidental destruction of data by employees, the introduction of computer viruses to the system, natural and human-made disasters, employees sharing passwords and misdirecting prints and distributing information to unauthorized people. The results highlighted that the greatest security concerns are perceived to come from within rather than from outside the business firms.

8/2 Impact of Cybersecurity on Organizations:

Cybersecurity incidents and breaches may have a significant effect on an organization . For example, breaches can result in lower performance, either operationally by reducing net income or impacting business value resulting in lower market value (Berkman et al.,2018) . In addition, cybersecurity incidents and breaches significantly affect investors decisions (Cheng &walton,2019) and affect operational factors such as service disruptions and loss of intellectual property.

Cybersecurity incidents and breaches can negatively impact the organization's reputation and result in devaluation of trade names lost customers , the study of (Curtis et al., 2018) focused on how security statement certainty and the behavioral intentions of potential consumers influence the perceptions of companies in the presence or absence of a past security breach. The findings indicated that the presence or absence of such a previous breach had a large impact on company perceptions but a minimal impact on behavioral intentions to be more secure personally. The findings implied that companies need to be cautious about how much confidence they convey to consumers. Cybersecurity incidents and breaches may also result in compliance challenges, attorney fees and litigation costs (Accenture , 2019).

On the other hand (Gordon et al., 2010) highlighted that the SOX of (2002) had a positive impact on the voluntary disclosure of information-security activities by business corporations. The findings indicated that the voluntary disclosure concerning cybersecurity had increased by over 100 percent since the passage of SOX compared with two years prior to the law's implementation. The study argued that voluntary disclosures in the annual report on cybersecurity allow a corporation to provide signals to the markets that the firm is actively engaged in preventing, detecting and correcting security breaches. So, that

firms taking proactive action have an incentive to disclose information related to cybersecurity risk management truthfully.

As mentioned earlier, the study provided empirical evidence that voluntary disclosures related to cybersecurity are positively and significantly related to the stock price. The results also indicated that managers who disclose information voluntarily are consistent with increasing firm value. Most importantly, their results showed that voluntary disclosures related to proactive security measures by a firm have the greatest impact on the firm's market.

In addition, (Li et al., 2018) investigated whether cybersecurity risk disclosure is informative for future cybersecurity incidents. The study found that the presence of risk factors in the pre-guidance period and the length of these risk factors are related to future reported cybersecurity incidents. However, the findings indicated that the association between the presence of cybersecurity risk disclosure and subsequently announced cybersecurity incidents become insignificant after the passage of the (SEC) cybersecurity disclosure guidance. (Carré et al., 2018) examined consumer reactions to security breaches and sought the best approach for companies to minimize reputational damage, because customers viewed that companies are more responsible for data protection.

8/3 Responses to Detected Cybersecurity Threats, Incidents, and Breaches:

Different parties respond to detected cybersecurity incidents and breaches in different ways. The Event, Impact, Response approach examines how four specific parties - management, investors, auditors, and regulators – respond to detected incidents and breaches.

8/3/1 Management Response:

Management can enhance cybersecurity by integrating general concepts from enterprise risk management with recent

cybersecurity reporting and assurance guidance from the (AICPA, 2017a, 2017b). Table (1) can be characterized as the stages of an effective cybersecurity risk management program. Although Table 1 represents these stages as discrete steps, they should be performed continuously and repeatedly as new cybersecurity risks continually arise. The first three stages are foundational to any effective risk management program, where the organization (1) identifies and prioritizes its risks/exposures, (2) designs and implements relevant controls to mitigate the risks/exposures, and (3) monitors the operating effectiveness of the controls in mitigating the risks/exposures.

The final two stages represent the AICPA's (2017a, 2017b) recent guidance on cybersecurity reporting and assurance, which is designed to address external stakeholders' concerns with the reporting organization's cybersecurity risk management. In the reporting stage, the (AICPA ,2017a) has issued description and control criteria to facilitate management's preparation of consistent external cybersecurity reporting. In the assurance stage, reporting organizations can foster the credibility of their cybersecurity reporting by procuring independent assurance of their description and control criteria. To facilitate the provision of this assurance service, the AICPA (2017b) has issued cybersecurity attestation criteria. Table (1) describes steps to enhance cybersecurity efforts within each stage.

TABLE 1

Stages of Effective Cybersecurity Risk Management

1. Cybersecurity risk/exposure identification and prioritization	Accounting firms can help companies identify and prioritize cybersecurity risks/exposures by leveraging their IT expertise and knowledge of current cybersecurity threats.
2. Cybersecurity control system design	Accounting firms can help companies design cybersecurity controls to address the risks/exposures identified in Stage 1. Accounting firms possess considerable IT control system expertise, including current industry best practices and control standards (e.g., AICPA's Cybersecurity Control Criteria).
3. Testing the operating effectiveness of cybersecurity controls	Accounting firms can test the operating effectiveness of companies' cybersecurity controls in either advisory or assurance capacities. Accounting firms have extensive experience in testing IT controls in conjunction with their financial statement audits and IT advisory services. If not part of externally reported assurance, this advisory service would be considered internal auditing.
4. External cybersecurity reporting	Accounting firms can help companies prepare external cybersecurity reports in accordance with external criteria (e.g., the AICPA's entity-level cybersecurity reporting framework).
5. Assurance on external cybersecurity reporting	Advisory: Accounting firms can help companies prepare for and assess their readiness for a formal assurance engagement regarding the effectiveness of a company's cybersecurity risk management program. Readiness assessments should be based on successful completion of Stages #1–4. Assurance: Accounting firms can provide a formal assurance engagement regarding the effectiveness of a company's cybersecurity risk management program. Assurance reports may or may not be shared publicly. If shared publicly, the accounting firm should not have provided any advisory services in Stages 1–4, for independence purposes.

So, all business firms should have effective cybersecurity risk management programs to increase the trust and the transparency of financial reports in the context of Industry 4.0.

(a) Cybersecurity Risk / Exposure Identification and Prioritization:

Risk identification and prioritization is essential for effective risk management. If a company fails to identify certain risks or prioritizes the wrong risks, risk management is bound to fail and result in significant adverse consequences. This is especially true in cybersecurity, where there are many and ever-changing cybersecurity threats devised by hackers.

As keeping current on cybersecurity threats is challenging for companies, accounting firms' consulting services are dedicated to keep abreast of new and emerging cybersecurity threats and communicating them to their clients. In addition, accountants with auditing backgrounds have significant expertise in risk

assessment, making them well-positioned to assess the likelihood and magnitude of the various threats for risk prioritization purposes based on the exposures and vulnerabilities within their client's business. High-quality IT risk assessments are critical in identifying the areas in the system that may be vulnerable to data breaches.

Cybersecurity risk assessments should be regularly reviewed at both the board and Audit Committee levels thereby ensuring that responsibility and accountability are clearly understood and that the level of threat is appropriately managed with sufficient resources. In assessing cyber risk across the organization there are several factors that need to be considered :

• identifying the assets that require protection; this should emphasise those that have the greatest strategic value to the organization .

- identifying relevant threats and weaknesses.
- identifying exploitable vulnerabilities.
- assessing the level of threat posed by those accessing the organisation's systems remotely.
- determining the business impacts if the threats are realized .
- developing a security-risk assessment.
- assessing the level of risk acceptance that is appropriate to the organization.
- identifying suitable control mechanisms to implement. In some cases, especially for smaller entities, some level of external advice may be appropriate in undertaking this assessment.

Deep risk analysis enable management not only to assess the detailed business impact of each type of cybersecurity attack, but also to understand where and how enabling security technologies can make a difference. Armed with this knowledge, organizations can better guide their security investments toward technologies

with the largest potential cost savings. Further, they can focus those technologies on the internal activities with the greatest strategic impact on improving cybersecurity protection.

(b) Cybersecurity Control System Design:

After identifying cybersecurity risks, the next stage is to design effective controls to mitigate the risks. Accountants have a significant competitive advantage in this stage due to their expertise in internal control. Also, auditors have significant experience identifying and evaluating internal controls that have financial reporting implications, including IT controls over the accounting-related systems and general controls over the IT function. Auditors also assess business process controls under the latest technologies, including those that can enhance cybersecurity controls, such as blockchain, cloud computing , security advanced authentication and built-in encryption.

Due to the complexity and rapid rate of innovation, it is challenging for companies to keep up with these innovations and ensure that they are utilizing. Accountants are well-positioned to develop a plan to design cybersecurity controls based on the exposures identified in the cybersecurity risk assessment stage. Thus, a control system should define a few remote access methodologies with sufficient security controls and block any unauthorized remote access technologies.

(c) External Cybersecurity Risk Management Reporting:

The American Institute of Certified Public Accountants (AICPA, 2018a) stated that “Cybersecurity is one of the top issues on the minds of management and boards in nearly every company in the world , large and small, public and private.” Therefore, it is extremely important that every organization consider a cybersecurity risk management program. In addition, certain organizations and their stakeholders need timely, useful

information about organizations' cybersecurity risk management efforts.

Accordingly, the (AICPA, 2018a) highlighted that cybersecurity is not just an information technology (IT) problem; it is an enterprise risk management problem that requires a global solution. The (AICPA, 2018b) also emphasized the importance of the entity-level cybersecurity reporting framework. It explicitly stated that the goal of the reporting framework is to provide a means by which organizations can communicate useful information regarding their cybersecurity risk management programs to stakeholders. Hence, the reporting framework is used to perform an examination-level attestation engagement.

The cybersecurity report should includes three key sets of information: (1) the management's description; (2) the management's assertion; and (3) the practitioner's opinion. To conclude, the AICPA (2018b) emphasized that its cybersecurity risk management reporting framework is a crucial first step toward enabling companies to communicate successfully with key stakeholders on how they are managing cybersecurity risk. In addition, the Securities and Exchange Commission (SEC) (2018, p. 4) argued that it is essential that Public companies take all required actions to inform investors about material cybersecurity risks and incidents in a timely fashion, including those companies that are subject to material cybersecurity risks but may not yet have been the target of a cyber-attack.

As mentioned, in response to stakeholders' demand for more information from companies on cybersecurity, the AICPA recently issued a voluntary reporting and assurance framework as a means for companies to communicate their cybersecurity risk management efforts to interested stakeholders (AICPA, 2017; Tysiac, 2017). This reporting is indeed voluntary as it goes beyond the SEC requirements to report material cybersecurity risks, incidents, and related controls. The reporting entails a narrative

description of the company's cybersecurity risk management program, management's assertions as to the description's compliance with the guidelines set forth by the AICPA, and whether the cybersecurity controls were operating effectively during the reporting period.

As accountants' core competency is external reporting, they have the skills to help companies prepare the narrative description. In addition, their expertise in control testing can inform management's assessment of the operating effectiveness of cybersecurity controls. With respect to companies who have experienced cybersecurity incidents, recent research suggests that external cybersecurity reporting can help restore investor confidence when coupled with assurance (Frank et al. 2019). Thus, companies that have experienced prior cybersecurity incidents should consider external cybersecurity reporting such as the AICPA Framework. In fact (Frank et al., 2019) find that external cybersecurity reporting also promotes investor confidence for firms that have not experienced cybersecurity incidents. These results demonstrate the value of external cybersecurity reporting as a means to address investors' significant cybersecurity concerns across all public companies, not just those that have experienced incidents . Also, (Islam et al., 2018) points out that managing cybersecurity risks is increasingly important for companies because of the growing dependence of firms on technology for conducting their business, creating a competitive advantage and achieving success.

(d) Assurance on External Cybersecurity Reporting :

With the reporting guidance, the AICPA also issued an attestation guide for companies that desire to have their cybersecurity report independently assured. Such assurance over cybersecurity risk management is broader than the traditional assurance engagements, which cover narrower aspects of IT controls for service organizations. In fact, beyond financial statement auditing,

accounting firms have been providing other forms of assurance, including assurance over IT controls. Auditors not only have assurance expertise, but also the expertise to effectively evaluate the effectiveness of companies' cybersecurity risk management. As mentioned, when a firm has experienced a prior cybersecurity incident, research indicates that independent assurance is necessary for external cybersecurity reporting to improve investor confidence (Frank et al. 2019). Thus, firms that have experienced cybersecurity incidents should be cautious of investing in external cybersecurity reporting without the enhanced credibility from independent assurance.

In addition, several studies discussed the cooperation between internal auditing and information-security functions. In many companies, both of them are involved with cybersecurity risk management . For instance, (Steinbart et al., 2012) argued that these functions should work together synergistically, because the information security staff designs, implements, and operates various procedures and technologies to protect the organization's information resources, and internal audit provides periodic feedback concerning effectiveness of those activities along with suggestions for improvement.

Also, (Steinbart et al., 2018) conducted a study investigated the influence of a good relationship between the two functions on information-security outcomes. In other words, the study investigated how the quality of the relationship objectively measures the overall effectiveness of an organization's information-security efforts. The findings highlighted that the quality of the relationship has a positive effect on the number of reported internal control weaknesses and incidents of non-compliance as well as on the number of security incidents detected, both before and after they caused material harm to the organization. Finally, the study emphasized that higher levels of management support for information security and having the chief

information security officer (CISO) report independently of the IT function have a positive effect on the quality of the relationship between the internal audit and information security functions.

Similarly, (Stafford et al., 2018) examined the role of information-security policy compliance and information system auditing in identifying non-compliance in working environments. Their findings indicated that enterprise risk management (ERM) benefits from audits that identify technology users who might feel invulnerable to cyber threats. Moreover, the study concluded that the internal audit has valuable role to assess and consult, to improve cybersecurity risk management in the firm. (Islam et al., 2018) added that cybersecurity auditing is a relatively new dimension of security practice intended to support the protection of critical information assets , and the audit process will seek to obtain evidence of organizational cybersecurity policies and their efficacy for the protection of asset integrity, data confidentiality and data access and availability.

8/3/2 Investors Response:

Investors may adjust their investment decisions and react to detected cybersecurity breaches by lowering the probability of investment or offering less money to purchase stocks (Deloitte, 2018 ; 2019). In contrast, market participants may view publicly disclosed cybersecurity breaches in a positive light as they respect the fact that the organization's management is willing to make this voluntary disclosure. Finally, investors may respond to cybersecurity breaches that are not appropriately or timely disclosed by initiating lawsuits.

8/3/3 Auditors Response:

When cybersecurity threats are acknowledged, external and / or internal auditors may work with management as consultants to address these concerns. Further, when cybersecurity incidents and breaches are detected, both internal and external auditors may

respond by increasing their efforts. External auditors may charge higher fees and / or perform additional engagements such as reviewing specific cybersecurity controls or engaging in a cybersecurity risk management examination (AICPA, 2018a). Finally, auditors may sue an organization if they suspect that its management knew of critical cybersecurity information but purposely did not disclose this information to the auditors.

8/3/4 Regulators Response:

Regulators may respond to cybersecurity events acknowledged by encouraging the organization to disclose its cybersecurity risk assessment activities (American Institute of CPAs 2018). Further, regulators may respond to detected breaches by imposing fines or additional reporting requirements. Finally, similar to investors, regulators may sue the organization to recover the costs incurred due to cybersecurity breaches.

8/4 The Importance of Cyber Risk Governance and Cyber Resilience :

Most organizations deal with cybersecurity from a tactical, threat-based level, rather than seeing it as a strategic risk. As a result, regular and incident based reporting often fails to reach board level . This can lead to a false sense of security even though the risks and vulnerabilities such as poor password policies or sharing of data with third parties have never been checked and are not reviewed from a business perspective. A further danger is a siloed approach , where the board make individuals responsible for data security, finance and so on but no one is taking a systematic and holistic view of the company’s exposure to cyber risk via its various IT systems and networks, its information assets, its digital connections and its people and working culture. Good cyber governance means looking at the entire data lifecycle and the various uses to which data is put.

It is important that organizations have a robust approach to cyber governance. This should be part of the overall business risk management processes. The board responsibility for good cybersecurity risk management begins with boards recognizing that cybersecurity is primarily a business risk and the Chief Financial Officer (CFO) is the best person to help quantify the financial and reputational impact of that risk and ensure that countermeasures are appropriate and cost-effective. Boards need to apply the key principles of visibility, accountability and responsibility to their cybersecurity strategies. Organisations that have a Chief Risk Officer (CRO) should consider the accountability line for the management of cyber risk. They need to have an overall view of the risk and therefore work closely with the CIO, the marketing teams and the CIO / IT manager as well as finance. In organizations without this role it is important that the finance leadership adopt a similar role. The CRO should also be responsible for monitoring the progress of cyber investments as well as continual assessments of the effectiveness of the controls in place to minimize the risks.

As the cyber threat has moved from being isolated to more pervasive, so organizations need to rethink their approach and, rather than focusing on the prevention of breaches, they need to focus on resilience. Cyber resilience combines the aspects of traditional disaster recovery planning and business continuity management so that the organization becomes agile in its responses. The ability to react quickly can help in limiting the financial and reputational damage. There are four stages in establishing cyber resilience as shown in figure 6 below :

(a) Manage and Protect :

This stage focuses on managing the data and assets in the information systems and networks. It establishes policies for protecting the organisation from cyber-attack, system failures and unauthorised access. This involves establishing defences that cover people, processes and technology.

(b) Identify and Detect :

In this stage, the vulnerabilities of the organisation are identified and protected by using techniques such as security tests, vulnerability scans and intrusion detection.

(c) Respond and Recover :

This stage includes the business continuity plans and incident response measures.

(d) Govern and Assure :

At this stage, the organisation should review its compliance with legal and regulatory requirements. This should involve a regular

risk assessment and a continuous improvement programme.

Figure 6 : Stages in Cyber Resilience

9/ Conclusion :

Due to recent increased cybersecurity threats and breaches, organizations are under pressure to consider the accounting implications of these attacks and develop appropriate responses. Specifically, cybersecurity events may affect organizations' operations, financial and non-financial performance, and ultimately its stakeholders. To address how cybersecurity issues may affect accounting, this research presents a proposed framework based on the Event, Impact, Response approach to discuss implications of cybersecurity on Accounting Information to increase the trust and transparency of financial report in the Context of Industry 4.0. The Framework highlights how practitioners can better assess cybersecurity threats, understand their impact, and develop response strategies. Results encourage additional research examining how organizations identify cybersecurity threats, incidents, and breaches, and how management responses to cybersecurity risks. Further, the researches about cybersecurity need to be extended beyond the AIS to other areas such as financial accounting, managerial accounting, and auditing.

10/ Potential Research Opportunities:

Increasing interest in cybersecurity highlights the need for future insightful and impactful interdisciplinary cybersecurity research. Since cybersecurity can directly impact firms' financial reporting practices and stakeholders' perceptions, understanding cybersecurity becomes paramount, especially as cybersecurity incidents occur at an ever-increasing rate. Cybersecurity can impact controls, operational, reputational, compliance, and litigation risks, and a firm's corporate governance. Future research could provide managerial insights and policy implications that improve our understanding and management of cybersecurity. Additionally, research can identify cybersecurity solutions and explain individual and firm behavior. In this section, we use our topical organization framework to guide the discussion of future research opportunities. While this paper provides a starting point for identifying future opportunities, we encourage further cross-topic research. Further, underscoring each of these issues is the need for additional studies focuse on broadening our ability to instill students with a robust understanding of the growing role of cybersecurity in firms.

This paper is just one step in an extended process to examine how cybersecurity impacts accounting information. More work is needed to improve how data incidents and breaches are detected and to reduce the probability that data incidents and breaches occur. Further, management response to cybersecurity breaches requires additional exploration. While some studies have examined how investors react to cybersecurity breaches, more work in understanding investors, auditors, and regulators behavior would be helpful.

future research needs to broadly consider the determinants of cybersecurity disclosures including industry and firm characteristics, regulations, and management incentives. Both industry and firm characteristics could provide specific evidence on disclosure determinants. Additionally, research could investigate which industry and firm characteristics, such as the prior disclosure of an internal control weakness, are associated with meaningful disclosures. Additionally, research should investigate how corporate governance and management incentives affects cybersecurity disclosure.

11/ References :

Abu-Musa, A.A. (2006), "Perceived security threats of computerized accounting information systems in the Egyptian banking industry", Journal of Information Systems, Vol. 20 No. 1, pp. 187-203.

Accenture. 2016. The Convergence of Operational Risk and Cyber Security.

Accenture. 2019. The cost of cybercrime. Available at: https://www.accenture.com/_acnmedia/pdf-96/accenture-2019-cost-of-cybercrime-study-final.pdf.

American Institute of Certified Public Accountants (AICPA). 2017. SOC for Cybersecurity: Helping You Build Trust and Transparency. Durham, NC: AICPA. Available at: https://www.aicpa.org/content/dam/aicpa/interestareas/frc/assuranceadvisoryservices/ downloadabledocuments/soc-for-cybersecurity-brochure.pdf

American Institute of Certified Public Accountants (AICPA, 2018a), "Cybersecurity risk management reporting fact sheet", available at: www.aicpa.org/content/dam/aicpa/ interestareas/frc/assuranceadvisoryservices/downloadabledocuments/cybersecurity-factsheet. pdf (accessed 13 November 2018).

American Institute of Certified Public Accountants (AICPA,2018b), "SOC for cybersecurity: a backgrounder", available at: www.aicpa.org/content/dam/aicpa/interestareas/frc/ assuranceadvisoryservices/downloadabledocuments/soc-for-cybersecurity-backgrounder. pdf (accessed 13 November 2018).

Amir, E., Levi, S. and Livne, T. (2018), "Do firms underreport information on cyber-attacks? Evidence from capital markets", Review of Accounting Studies, Vol. 23 No. 3, pp. 1177-1206.

Banker, R., and C. Feng. 2019. The impact of information security breach incidents on CIO turnover. Journal of Information Systems 33(3): 309–329. https://doi.org/10.2308/isys-52532

Berkman, H., Jona, J., Lee, G. and Soderstrom, N. (2018), "Cybersecurity awareness and market valuations", Journal of Accounting and Public Policy, Vol. 37 No. 6, pp. 508-526.

Boritz, J.E. and No, W.G. (2005), "Security in XML-based financial reporting services on the internet", Journal of Accounting and Public Policy, Vol. 24 No. 1, pp. 11-35.

Cheng, X., and S. Walton. 2019. Do nonprofessional investors care about how and when data breaches are disclosed? Journal of Information Systems 33 (3): 163–182. https://doi.org/10.2308/isys-52410

Cheng, X., and T. Wang. 2019. Talk too much? The attribution of cybersecurity disclosures on investment decisions. Working Paper, Auburn University and DePaul University.

COSO. 2017. *Enterprise Risk Management Framework: Integrating with Strategy and Performance*. . https://www.coso.org/Documents/COSO-ERM-Presentatio.

Curtis, S., Carre, J. and Jones, D. (2018), "Consumer security behaviors and trust following a data breach", Managerial Auditing Journal, Vol. 33 No. 4, pp. 425-435.

Deloitte. (2016a). Response to the proposed description criteria for management's description of an entity's cybersecurity risk management program. Retrieved from https://dart.deloitte.com/USDART/ov-resource/139e0012-c07f-11e6-a391-2b48717272bf.pdf

Deloitte. (2016b). Cyber crisis management: Readiness, response, and recovery. Deloitte. Available at : https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Risk/gx-cm-cyberpov. pdf

Deloitte. (2018). Focusing the lens on cyber reporting: The AICPA cybersecurity risk management examination one year later. Retrieved from https://www2.deloitte.com/content/dam/Deloitte/us/Documents/risk/us-advisory-cybersecurity-risk-management-examination.pdf

Deloitte. (2019). Hidden Business Impact of Cyberattack. https://www2.deloitte.com/us/en/pages/risk/articles/hidden-business-impact-of-cyberattack.html.

Forbes. 2017. The Top Cyber Security Challenges Experts Are Facing Today. Forbes. Accessed May 30, 2019. https://www.forbes.com/sites/quora/2017/05/31/the-top-cyber-security-challenges-expertsare- facing-today/#7c5bb1992238.

Frank, M., J. Grenier, and J. Pyzoha. 2019. How prior cyberattacks influence the efficacy of cybersecurity risk management reporting and

Gordon, L.A., Loeb, M.P. and Sohail, T. (2010), "Market value of voluntary disclosures concerning information security", MIS Quarterly, Vol. 34 No. 3, pp. 567-594.

Gordon, L.A., Loeb, M.P., Lucyshyn, W. and Zhou, L. (2015a), "The impact of information sharing on cybersecurity underinvestment: a real options perspective", Journal of Accounting and Public

Gordon, L.A., Loeb, M.P., Lucyshyn, W. and Zhou, L. (2015b), "Externalities and the magnitude of cybersecurity underinvestment by private sector firms: a modification of the Gordon-Loeb model", Journal of Information Security, Vol. 6 No. 1, pp. 24-30.

Gordon, L.A., Loeb, M.P., Lucyshyn, W. and Zhou, L. (2018), "Empirical evidence on the determinants of cybersecurity investments in private sector firms", Journal of Information Security, Vol. 9 No. 2, pp. 133-153.

Gordon, L.A., Loeb,M.P. and Zhou, L. (2011), "The impact of information security breaches: has there been a downward shift in costs?", Journal of Computer Security, Vol. 19 No. 1, pp. 33-56.

Haopamaki, E and sihvonen , J " cyber security in accounting research" Managerial Auditing Journal 2019, Vol34, no.7,pp.808-834

Institute of Internal Auditors (IIA) (2018), "The future of cybersecurity in internal audit. A joint research report by the internal audit foundation and crowe horwath", available at: https:// bookstore.theiia.org/the-future-of-cybersecurity-in-internal-audit.

Islam, M.S., Farah, N. and Stafford, T.S. (2018), "Factors associated with security/cybersecurity audit by internal audit function: an international study",Managerial Auditing Journal, Vol. 33No. 4, pp. 377-409.

Janvrin, D and wang. T "Implication of Implication of cyber security an Accounting Information" Journal of Information systems, September 2019, Vol. 33, No.3 pp.A,A2

Janvrin, D, and Wang , T " linking cyber security and Accounting: Prevent impact. Response Framework" Accounting Harizon, september, 2021.

Li, H., No, W. and Wang, T. (2018), "SEC's cybersecurity disclosure guidance and disclosed cybersecurity risk factors", International Journal of Accounting Information Systems, Vol. 30, pp. 40-55.

Muravskyi, V Accounting and cyber security ongraph kindle publishing, KDP, December, 2021.

Muravskyi, V" the Accounting system as the Basis for organ sing Enterprise cyber security " Financial and credit activity " Financial and credit Activity problems of theory and practice September, 2020

Ponemon Institute. (2017). 2017 Cost of cyber crime study. Retrieved from https://www.ponemon.org/blog/2017-cost-of-cyber-crime-study

PricewaterhouseCoopers. (2016). PwC comments on ASEC's proposed revision of its trust services criteria. Retrieved from https://www.pwc.com/us/en/cfodirect/publications/comment-letter-aicpa/aicpa-asec-proposed-revision-trust-services-criteria.html

PricewaterhouseCoopers. (2017). The Global State of Information Security® Survey 2018. Retrieved from https://www.pwc.com/us/en/services/consulting/cybersecurity/library/information-security-survey.html

Public Company Accounting Oversight Board (PCAOB). 2018. Strategic plan 2018–2022. Available at: https://pcaobus.org/About/Administration/Documents/Strategic%20Plans/PCAOB-2018-2022-Strategic-Plan.pdf.

Richardson, V., R. Smith, and M. Watson. 2019. Much ado about nothing: The (lack of) economic impact of data privacy breaches. Journal of Information Systems 33 (3): 227–265. https://doi.org/10.2308/isys-52379.

Securities and Exchange Commission (SEC) . 2017. *Statement on cybersecurity*. Securities and Exchange Commission.

Securities and Exchange Commission (SEC) .2018. "Commission statement and guidance on public company cybersecurity disclosures", available at: www.sec.gov/rules/interp/2018/33-10459.pdf.

Stafford, T., Deitz, G. and Li, Y. (2018), "The role of internal audit and user training information security policy compliance", Managerial Auditing Journal, Vol. 33 No. 4, pp. 410-424.

Steinbart, P.J., Raschke, R., Gal, G.F. and Dilla, W.N. (2012), "The relationship between internal audit and information security: an

exploratory investigation", International Journal of Accounting Information Systems, Vol. 13 No. 3, pp. 228-243.

Steinbart, P.J., Raschke, R.L., Gal, G. and Dilla, W.N. (2018), "The influence of a good relationship between the internal audit and information security functions on information security outcomes", Accounting, Organizations and Society, in press.

The World Bank (2018), "Financial sector's cybersecurity: regulations and supervision", available at: http://documents.worldbank.org/curated/en/686891519282121021/pdf/123655-REVISED-PUBLICFinancial- Sectors-Cybersecurity-Final-LowRes.pdf

Tysiac, K. (2017). A new cybersecurity risk management reporting framework for management and CPAs. *Journal of Accountancy*, retrieved on October 1, 2020, from https://www.journalofaccountancy.com/news/2017/apr/cybersecurity-risk-management-reporting-framework-201716483.html.

Walton, S, wheeler, P, zhang, y and zhao, x " An integrative review and analysis of cyber security Research: current state and Futune Directions Journal of Information systems, spring 2021, vol, 35, No.1 PP.155-186

Walton, S, wheeler, P, zhang, y and zhao, x" An Integrative Review and analysis of cyber security research: Current state and Future Directions: Journal of Information systems, spring 2021, Vol 35, no.1, pp.155-185.

Walton, S., P. Wheeler, Y. Zhang, and X. Zhao. 2020. An integrative review and analysis of cybersecurity research: Current state and future directions. *Journal of Information Systems* 35 (1): 155-186.

Werner, R. R. 2017. How to protect common cyberattacks and insure against potential losses. *The CPA Journal* March: 17-21.

Willison, R., Warkentin, M., & Johnston, A. C. (2018). Examining employee computer abuse intentions: Insights from justice, deterrence and neutralization perspectives. *Information Systems Journal*, *28*(2), pp. 266–293.

Xu, H., S. Guo, J. Haislip, and R. Pinsker. 2019. Earnings management in firms with data security breaches. *Journal of Information Systems* 33 (3): 267-284. https://doi.org/10.2308/isys-52480.