INFLUENTIAL FACTORS IN INDUSTRIAL CYBERSECURITY: A SYSTEMATIC LITERATURE REVIEW AND ROADMAP FOR FUTURE RESEARCH

Lappeenranta–Lahti University of Technology LUT

Master’s thesis

M.Sc Software Engineering and Digital Transformation

2023

Siva Gopi Chinka

Examiner(s): Professor Najmul Islam PhD

Prabhat Kumar, Post-doctoral researcher
ABSTRACT
Lappeenranta–Lahti University of Technology LUT
LUT School of Engineering Science
Software Engineering and Digital Transformation

Siva Gopi Chinka

INFLUENTIAL FACTORS IN INDUSTRIAL CYBERSECURITY: A SYSTEMATIC LITERATURE REVIEW AND ROADMAP FOR FUTURE RESEARCH

Master’s thesis
2023
48 pages, 4 figures, 4 tables and 00 appendices
Examiner(s): Professor Najmul Islam, PhD and Prabhat Kumar, Post-doctoral researcher
Keywords: Influential factors, Cybersecurity, Social, Environmental, Economic, Technological.

With increased application of technology in organizations, cyber-security has become an important factor as cyber-threats grow in number and become sophisticated. It is for this reason that governments and business organizations have invested considerably in cyber-security. However, despite the attention cyber-security has received over the years, it remains a challenge as reflected in the significant number of cyber-incidents. This paper thereby focused on examining the factors influencing industrial cyber-security with a view of determining how these factors have contributed to the success or failure of cyber-security efforts. To find answers, using a systematic literature review, we identified 4579 studies, out of which 40 articles were summarized. From the review, four main factors were identified and these are social, economic, technological, and environmental factors. The main social factors identified from the selected sources are human factors and regulatory compliance. It was established that human factors like knowledge and skills, negligence, behaviour, and attitude have affected the adoption and implementation of cyber-security in many organizations. In relation to compliance, the regulatory framework is too complex or people are not compelled to comply with cyber-security regulations. The main economic factor is resource availability while the technological factors are technological advancements and development of new cyber-attack methods. Resource constraints are the main environmental factor. This paper contributes to industrial cyber-security literature by highlighting influential factors affecting cyber-security and the research gaps in existing literature. The findings in this paper can guide the cyber-security strategies adopted by governments and organizations around the world.
ACKNOWLEDGEMENTS

I am really grateful to Professor Najmul Islam for his invaluable assistance and guidance, as well as Prabhat Kumar. His experience in the topic and enlightening discussions have greatly aided the development of this thesis. Finally, I'd want to thank my parents and friends for their unwavering support, motivation, and encouragement throughout my life; I wouldn't be here without them. They are my biggest source of motivation in my career.

Siva Gopi Chinka
ABBREVIATIONS

AI       Artificial Intelligence
IOT      Internet of things
CRs      Cyber-Ranges
TBs      Test-Beds
WOS      Web of Science
SLR      Systematic Literature Review
Table of contents

Abstract

(Acknowledgements)

(Abbreviations)

1 Introduction ............................................................................................................. 10
  1.1 Background and motivation for the study ......................................................... 10
  1.2 Research questions and objectives .................................................................. 11
  1.3 Scope of the study ......................................................................................... 12
2 Research method ................................................................................................... 13
  2.1 Selecting Databases ....................................................................................... 13
     2.1.1 Search terms and keywords used ......................................................... 13
     2.1.2 Search result extraction and analysis .................................................. 14
  2.2 Inclusion and Exclusion Criteria ..................................................................... 15
     2.2.1 Search timeline ..................................................................................... 16
  2.3 Selection Strategy ............................................................................................ 16
     2.3.1 Data extraction process ........................................................................ 17
     2.3.2 Data analysis ......................................................................................... 17
3 Literature review results ...................................................................................... 20
  3.1 Influencing factors of Industrial Cybersecurity ............................................. 20
  3.2 Social Factors .................................................................................................. 21
     3.2.1 Human-related factors .......................................................................... 21
     3.2.2 Regulatory and policy compliance ...................................................... 25
  3.3 Economic Factors ............................................................................................ 27
  3.4 Environmental Factors .................................................................................... 29
  3.5 Technological Factors ...................................................................................... 30
4 Comprehensive Framework .................................................................................... 33
5 Research gaps and future research directions .................................................... 35
  5.1 Lack of research on Physical environment ................................................... 35
  5.2 Solutions to emerging cyber-threats ................................................................. 35
5.3 Limited empirical evidence

6 Discussion

6.1 Key findings

6.2 Practical Implications

6.3 Research Implications

7 Conclusion

7.1 Limitations

References
Figures

Figure 1: Article screening and selection process

Figure 2: Discipline of publication venue and number of selected studies by publication year

Figure 3: Thematic map of influential factors in industrial cybersecurity

Figure 4: Comprehensive framework for Industrial Cybersecurity and its factors explored in existing literature

Tables

Table 1: Search terms and results

Table 2: Inclusion and Exclusion criteria

Table 3: Number of Journals and Conference publications by year

Table 4: Top five cited articles based on Google Scholar
1 Introduction

Industrial cybersecurity has become crucial with the emergence of industry 4.0. Industry 4.0 is the fourth industrial revolution characterized by a high level of automation, use of smart technologies and systems, and application of big data. Industry 4.0 has resulted in the interconnected systems and sharing of data (Ustundag et al., 2018). The problem is this has led to a high risk of cyber-security. A cyber-attack on a part of the system can lead to the collapse of the whole system. For instance, introduction of malware at one point can result in the spread of the virus to all other parts (Clim, 2019). The interconnected digital in the industry 4.0 era has also created numerous points of entry into a system for cyber-attackers. Industrial cyber-security is thereby critical in protecting digital systems against any attack.

Data is very important within the industry 4.0 framework. It is currently referred to as the new oil. Industries around the world are constantly collecting, generating, storing, and using data to make decisions on what to (Ustundag et al., 2018). Some of this data is sensitive and can harm organizations and individuals if accessed by unauthorized individuals. Industrial cyber-security is thereby necessary to make sure that the data is protected (Dawson, 2018).

1.1 Background and motivation for the study

In recent decades, cybersecurity has become increasingly important, particularly with technological advancements. The significance of cybersecurity is reflected in the number of cyber-incidents. (Hassanzadeh et al., 2020) indicate that between 2006 and 2019 the water sector in the US experienced more than 20 cybersecurity incidents. This is despite measures being taken after each incident. This is an indication that cyber-threats have been evolving over time. Hackers are constantly developing more sophisticated ways of intruding into systems.

The technological advancements which have resulted in the increased use of technology in many systems have increased the cyber-threat (Al-Mhiqani et al., 2018). For instance, technological advancement have led to emergence of cyber-physical systems which are digital systems comprising of physical and computational capabilities that engage with
humans (Al-Mhiqani et al., 2018). These systems connect computers, sensors, communication devices, and many other digital systems, forming a complex and interconnect network of systems. This has raised the cyber-security risk as access to one device opens the door to the whole interconnected system.

1.2 Research questions and objectives

The realization of the importance of cyber-security has led to enhanced research and investment in this area. However, cases of cyber-attacks continue to be rampant around the world, with organizations losing millions in some cases (Ustundag et al., 2018). While this is due to constant development of more sophisticated malware, there are possibly other factors that contribute to the situation. This paper aims to examine the influential factors in industrial cybersecurity. Many research have been undertaken to study the aspects that contribute to Industrial Cybersecurity and to propose options for resolution. Despite the development of such research, we have limited scope to acquire a thorough overview of Industrial Cybersecurity because existing literature tends to focus on only a restricted number of Industrial Cybersecurity features. A review-based study that summarizes previous research can help in this regard (Kitchenham and Charters, 2007; Tandon et al., 2020). As a result, we perform a systematic literature review (SLR) to synthesize the existing body of knowledge on Industrial Cybersecurity and give a comprehensive framework to guide future research (Kitchenham and Charters, 2007). Our SLR is guided by the following research questions (RQs): RQ1. What factors influence Industrial Cybersecurity? RQ2. What are the research gaps and limitations of the prior literature and what future research opportunities can be derived to advance the use of Industrial Cybersecurity?

The objectives of this thesis are:

- To examine the social factors impacting cybersecurity practices
- To identify the environmental factors affecting the resilience of cybersecurity in industrial facilities
- To determine the economic factors affecting cybersecurity
- To identify the technological factors influencing cybersecurity
To determine the implication of integrating emerging technologies such as AI and blockchain on industrial cybersecurity

1.3 Scope of the study

The review in this paper is limited to the influential factors in industrial cyber-security. The factors focused on are social, economic, environmental, and technological factors. The review will be limited to these factors. To address the research aims in this paper, 40 articles were selected and reviewed. The goal was to determine the factors highlighted by these sources as affecting industrial cybersecurity. The paper is structured in five main sections which are introduction, research method, results, discussion, and conclusion. The introduction provides a background to the study. The research method shows how data was collected and analysed. The results section presents findings obtained from reviewing the 40 sources identified. The discussion expounds on the results while the conclusion summarizes the results.
2 Research method

The research method applied in this paper is the systematic literature review. Systematic literature review is a method that identifies and evaluates relevant literature on a topic to draw conclusions on the question being considered (Kitchenham et al., 2009). In this case, the systematic literature review involves a search for sources that address influential factors in industrial cyber-security, reviewing the sources, and identifying what these sources indicate about the subject being researched.

2.1 Selecting Databases

The systematic literature review in this study began with identifying the databases that sources will be searched from. Two databases, Scopus and Web of Science (WOS), were identified as the most relevant (Burnham, 2006). A search of sources was focused in these two databases. The sources searched were those that examine the social, economic, environmental, and technological factors affecting industrial cybersecurity

2.1.1 Search terms and keywords used

The search terms and the results extracted are provided in Table 1. The search terms used are social factors in cybersecurity, economic factors in cybersecurity, environmental factors in cybersecurity, and technological factors in cybersecurity. The keywords used are industrial cybersecurity, social factors, environmental factors, economic factors and technological factors (Grames, Stillman, Tingley & Elphick, 2019). More specific terms such as human errors, budgetary constraints, resource availability, AI, IOT, block chain, regulatory framework, human factors in industrial cybersecurity, cybersecurity under technological advancements, and cybersecurity culture were used to get more relevant sources.
Table 1: Search terms and results

<table>
<thead>
<tr>
<th>Search terms</th>
<th>Database</th>
<th>Results</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Web of Science</td>
<td>1423</td>
</tr>
</tbody>
</table>

2.1.2 Search result extraction and analysis

The search for articles was carried out using the search terms and keywords. The search was limited to articles published in English language. The results from the two databases were then examined and the right articles selected. In situation where no relevant sources (Stoll et al., 2019) were obtained, keywords and terms were adjusted. From both databases, we considered only conference and journal articles, duplicates and Non-english articles were excluded and 450 articles were remained in the list. Exclusion criteria applied on the basis of reading the abstracts, 246 articles were removed from the list. Full texts of the remaining 204 articles were carefully reviewed in order to eliminate those that did not fall within the scope of our research theme. Furthermore, articles without empirical studies were removed, leaving the final 40 articles. Fig. 1 depicts the screening and selection process.
2.2 Inclusion and Exclusion Criteria

The first inclusion criterion is the relevance of the source. Only those sources that examine the social, economic, environmental, and technological factors influencing industrial cybersecurity were considered. Sources were also selected based on the date of publication. The most recently published sources were given priority because they are more relevant (Patino & Ferreira, 2018). For instance, sources published in 2022 and 2023 provide a more accurate picture of the cybersecurity situation in industries. Lastly, sources were selected based on publication type. In this study, peer-reviewed journal articles were prioritized. This
is because they are credible sources as they are evaluated by experts before being published (Meline, 2006). Most journal articles are based on empirical studies, meaning that the information therein is more factual. Conference papers were also considered. Sources that were excluded include those were published in a language other than English and articles that are not full-text. The inclusion and exclusion criteria are outlined in Table 2.

<table>
<thead>
<tr>
<th>Inclusion Criteria</th>
<th>Exclusion criteria</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Conference and peer-reviewed journal articles were included</td>
<td>1. Review articles, posters, presentations, book chapters, news, magazines and editorials were excluded</td>
</tr>
<tr>
<td>2. Only English-language publications were included</td>
<td>2. Articles published in languages other than English were excluded</td>
</tr>
<tr>
<td>3. Full-text content is available in online databases and repositories.</td>
<td>3. Non-Full-text studies were excluded.</td>
</tr>
<tr>
<td>4. There are articles with empirical studies were included</td>
<td>4. Duplicate studies were excluded.</td>
</tr>
</tbody>
</table>

2.2.1 Search timeline

The search for the sources we considered the studies that were published before October 2023. The search began by identifying the keywords and search terms and using them to search for sources from the selected databases. From them, the sources reviewed and the most relevant identified.

2.3 Selection Strategy

The first step in the selection process was examination of the title of a source. This was to determine whether the source is relevant and needed to be considered. The second step was examination of the abstract (Stoll et al., 2019). This was to get a general idea of what the article is addressing and whether it is within what is being sought for. The final step was
skimming through the whole article to determine if it meets the inclusion criteria. The most relevant articles were then selected.

2.3.1 Data extraction process

Data was extracted by reading through each article and identifying relevant information. For example, on articles that addressed social factors in industrial cybersecurity, these factors were identified and extracted (Munn, Tufanaru & Aromataris, 2014). Information from all the sources was then synthesized and presented in form of themes and sub-themes.

2.3.2 Data analysis

Data collected was analysed using thematic analysis (Munn, Tufanaru & Aromataris, 2014). Information from all the sources was then synthesized and presented in form of themes and subthemes.

Table 3: Number of journals and conference publications by year

<table>
<thead>
<tr>
<th>Publication year</th>
<th>Journals publications</th>
<th>Conference publications</th>
</tr>
</thead>
<tbody>
<tr>
<td>2014</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>2015</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>2017</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>2018</td>
<td>8</td>
<td>2</td>
</tr>
<tr>
<td>2019</td>
<td>3</td>
<td>0</td>
</tr>
<tr>
<td>2020</td>
<td>4</td>
<td>2</td>
</tr>
<tr>
<td>2021</td>
<td>5</td>
<td>1</td>
</tr>
<tr>
<td>2022</td>
<td>5</td>
<td>0</td>
</tr>
<tr>
<td>2023</td>
<td>7</td>
<td>0</td>
</tr>
</tbody>
</table>
This table highlights the number of sources under each year. For example, from the 40 sources, only one was published in 2014 while seven were published in 2023.

Fig 2: Discipline of publication venue and number of selected studies by publication year

This graph shows how many sources were published for each year. For example, 8 journal articles were published in 2018.

<table>
<thead>
<tr>
<th>Title</th>
<th>Year</th>
<th>Cited</th>
<th>Authors</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>On security challenges and open issues in Internet of Things</td>
<td>2018</td>
<td>251</td>
<td>Sha, K., Wei, W., Yang, T. A., Wang, Z., and Shi, W.</td>
<td>Journal</td>
</tr>
<tr>
<td>Title</td>
<td>Year</td>
<td>Citations</td>
<td>Authors</td>
<td>Journal</td>
</tr>
<tr>
<td>-----------------------------------------------------------------------</td>
<td>------</td>
<td>-----------</td>
<td>-------------------------------------------------------------------------</td>
<td>-----------</td>
</tr>
<tr>
<td>A comprehensive review study of cyber-attacks and cyber security;</td>
<td>2021</td>
<td>230</td>
<td>Li, Y., and Liu, Q.</td>
<td>Journal</td>
</tr>
<tr>
<td>Emerging trends and recent developments</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Human factor security: evaluating the cybersecurity capacity of the</td>
<td>2019</td>
<td>101</td>
<td>Ani, U. D., He, H. and Tiwari, A.</td>
<td>Journal</td>
</tr>
<tr>
<td>industrial workforce</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

This table shows the five sources which have been cited the most on Google Scholar.
3 Literature review results

As indicated sources were searched from two databases, Scopus and Web of Science. In this case, the systematic literature review involves a search for sources that address influential factors in industrial cyber-security, reviewing the sources, and identifying what these sources indicate about the subject being researched.

3.1 Influencing factors of Industrial Cybersecurity

The sources identified were reviewed based on four main factors which are social, economic, environmental, and technological factors influencing cybersecurity.

Fig 3: Thematic map of influential factors in industrial cybersecurity
3.2 Social Factors

The reviewed literature suggests that the main social factors influencing cybersecurity are human-related factors and regulatory and policy compliance. Under each factor there are sub-themes and under the sub-themes, there are further sub-themes. Each and every factor explained in detailed in below.

3.2.1 Human-related factors

The main social factors influencing cybersecurity are human-related factors. They include cybersecurity knowledge and skills, negligence, attitude and malicious intent (Yeng, Fauzi & Yang, 2022).

Knowledge and skills:

The reviewed literature shows that most people, especially in organizations, do not have adequate knowledge of cybersecurity (Ani, He & Tiwari, 2019; Singh & Singh, 2022; Pollini et al., 2022). People misunderstand or are ignorant of cybersecurity and information technology in general (Singh & Singh, 2022; Ani, He & Tiwari, 2019). In other words, people do not know what cybersecurity is and how important it is even though they have heard about it (Sawyer & Hancock, 2018). The lack of knowledge of cybersecurity makes people to engage in activities that put their systems in danger of cyberattacks (Hughes-Lartey, Li, Botchey & Qin, 2021). For example, people are quick to open suspicious email messages which provide access to their systems (Ani, He & Tiwari, 2019). Lack of knowledge is also demonstrated by people not understanding the basic terminologies in cybersecurity such as phishing, ransomware, and antivirus (Singh & Singh, 2022). Lack of knowledge has resulted in human errors that have contributed to data breaches.

In other cases, people are completely unaware of cybersecurity. In other words, they do not have any knowledge of cybersecurity, meaning that they can determine whether their system has been hacked or attacked (Sawyer & Hancock, 2018). Lack of awareness of cybersecurity makes it hard for people to take appropriate action whenever they suspect that their systems may have been attacked (Yeng, Fauzi & Yang, 2021). For instance, if the cursor on one’s computer begins moving on its own, it is an indication the computer is likely to have been
hacked and one may need to take appropriate action, including switching off the computer and trying to secure critical information (Singh & Singh, 2022). However, one may not bother to take any precautionary measure because of not being aware of the significance of risk faced (Yeo & Banfield, 2022).

In terms of skills, reviewed literature shows that in some cases, people have significant theoretical knowledge about cybersecurity but they do not have the same level of practical skills that could help them deal with cybersecurity situations (Ani, He & Tiwari, 2019). One of the reasons for limited skills in cybersecurity is because of lack of keenness for cybersecurity skills in industrial workforce. Few people are trained in cyber-security (Marotta & Madnick, 2021; Kabanda, Tanner & Kent, 2018). In other cases, the companies only hire cybersecurity specialists rather than educate the workforce on cyber-security (Mierzwa & Scott, 2017). As such, other employees do not attempt to learn how to deal with cybersecurity threats, which include taking preventive measures such as constantly changing the password or creating stronger passwords for their systems (Singh & Singh, 2022). Few individuals also engage in cybersecurity practices such as installing security plugins and updating their personal devices which are key to protecting their devices against cyber-attacks (Ani, He & Tiwari, 2019). In general, the key skills that are limited among people and which are critical to cybersecurity are credentials management which include creating and protecting passwords, malware detection and management, and email security, and patch management (Jalali & Kaiser, 2018). The lack of knowledge and skills are weaklinks that make systems conscious targets for attacks. Limited knowledge and skills is the leading human vulnerability that contributed to cyber-attacks (Ani, He & Tiwari, 2019). For instance, 20% of security breaches are attributed to misuse of infrastructure assets and 31% are because of human errors which are a consequence of limited knowledge and skills (Ani, He & Tiwari, 2019). Limited knowledge and skills have led stolen credentials through phishing, with 80% of data breaches being a consequence of such phishing (Ani, He & Tiwari, 2019).

Negligence:

Sources on human factors also indicate that negligence is a key factor that influences cybersecurity capability in organizations. A significant number of cases of cybersecurity issues have not evidence of malicious intent. Instead, they are characterized by employees or business associates engaging in risky behaviour that puts systems at a risk of cyberattacks
(Yeo & Banfield, 2022). For example, there are cases of misplaced hard drives among individuals that put sensitive information in danger of falling in wrong hands (Hughes-Lartey, Li, Botchey & Qin, 2021). There are also cases of protected information being emailed to wrong recipients. In other cases, protected information is emailed to the right individual but it is done in the manner that exposes the information (Yeo & Banfield, 2022). There are incidents where information was unintentionally exposed by individuals who uploaded it on publicly accessible databases or websites without taking appropriate security measures like sanitizing or encrypting data before uploading it (Catota, Morgan & Sicker, 2018). One of the impacts of negligence is it makes one prone to phishing or ransomware (Yeo & Banfield, 2022). This has led to systems being attacked as they are not well protected (Pollini et al., 2022). For instance, an individual may be sent a link and when they open it, it creates an avenue that allows the attacker to upload a virus or ransomware (Yeo & Banfield, 2022). This gives them access to the system.

**Malicious Intent:**

However, there are cases where individuals have malicious intent where they engage in activities that promote cybersecurity problems with the intention of benefitting financially or personally (Yeo & Banfield, 2022; Wilner et al., 2021; Yeng, Fauzi & Yang, 2021; Yeng, Fauzi & Yang, 2022). Other reasons why people may decide to maliciously attack or access sensitive information are they are disgruntled and thereby want to exact revenge for some wrong they feel was done unto them and they feel entitled and thereby attack their organization’s system if they feel that they have not been given the position they deserve (Yeo & Banfield, 2022). The malicious intent is in in form of cyber-attack or hacking, malicious insider, and theft or burglary (Yeng, Fauzi & Yang, 2022).

**Attitude:**

Attitude of individuals is also a key human factor affecting cybersecurity. Reviewed literature shows that many people, including IT personnel, have little attitude towards secure use of social networks (Pollini et al., 2022). In other words, the attitude towards cybersecurity is poor even those with knowledge about it. On the other hand, poor attitude contributes to risky information security-conscious behaviour (Yeng, Fauzi & Yang, 2021). Simply, having poor attitude towards cybersecurity makes people to act in the manner that puts information systems at a risk of being cyber-attacked. In addition, they do not take
any action that is aimed to prevent cybersecurity problems (Catota, Morgan & Sicker, 2019). For example, people take action only after experiencing security incidents. This affects cybersecurity readiness in that no proactive measures are taken to prevent cyber-security incidents (Catota, Morgan & Sicker, 2019). In the case of small scale business organizations, there is a feeling that they are less technologically complex and as such they do not face significant cyber-security threats. As such, they do not need to invest in cyber-security measures (Kabanda, Tanner & Kent, 2018).

**Human behaviour:**

The general human behaviour in relation to cybersecurity is one characterized by limited focus on preventing and dealing with cybersecurity problems (Sawyer & Hancock, 2018). Sources indicate that the detection of cyber-attacks is significantly low and this is because most people have not attempted to put in place strategies that would enable them to detect these attacks (Sawyer & Hancock, 2018). Even in situations where one has detected the attack, they are unlikely to report. The human behaviour in general is one where cybersecurity has not been given precedence. Other behaviours that contribute to cybersecurity include group sharing and borrowing (Watson, Moju-Igbene, Kumari & Das, 2020). Groups share resources such as digital media accounts and physical items, most of which are embedded with computation making them prone to cyberattacks (Watson, Moju-Igbene, Kumari & Das, 2020). People also borrow computing devices which also increase the risk of these devices being accessed by unauthorized individuals (Watson, Moju-Igbene, Kumari & Das, 2020).

**Education:**

Education is also a key factor that is aimed to deal with the human vulnerabilities in cybersecurity. Reviewed literature shows that the kind of education given has not helped to promote cyber-security (Catota, F. E., Morgan, M. G., & Sicker, D. C. (2019). One of the reasons why education has not helped improve cybersecurity according to sources reviewed in this study is lack of interaction between academia and industry (Catota, Morgan & Sicker, 2019). There is hardly any communication between the businesses and learning institutions such as universities. This means that academia does not understand that the industry demands in relation to cyber-security (Catota, Morgan & Sicker, 2019). This means that what is taught in school on cyber-security is not in line with cyber-security threats currently
faced (Catota, Morgan & Sicker, 2019). Another reason why education has been ineffective in promoting cyber-security is lack of cyber-security specialists. There are only a few educators with training in cybersecurity. This means that cybersecurity instruction does not equip learners with appropriate knowledge and skills. Most organizations also provide limited or no training to their employees on cyber-security (Mierzwa & Scott, 2017). It means that only a few employees have the knowledge and skills that enable them to deal with cyber-security issues.

In general, reviewed sources indicate that the human factor is a critical weak link that contributes to the cybersecurity challenges faced by organizations (Hughes-Lartey, Li, Botchey & Qin, 2021). The significance of the human factor in cybersecurity has led to concerted efforts to improve this aspect. For instance, reviewed literature shows that some organizations have cultivated the culture of collective responsibility when it comes to cybersecurity, where employees hold each other accountable (Watson, Moju-Igbene, Kumari & Das, 2020).

**Resistance to change:**

Some studies suggest that people are resistant to change and this reduces their intention to adopt cybersecurity measures. Some of the factors that contribute to resistant to change are job insecurity, perceived vulnerability, and perceived severity among others (Alneyadi & Normalini, 2023). If one perceives that they are likely to lose their job if cybersecurity measures are adopted, they resist any attempt to adopt these measures (Alneyadi & Normalini, 2023). On the other hand, if people perceive that their organization is not vulnerable to cyber-attacks and that in the case of attacks, the impact is minimal their intention to adopt cybersecurity reduces (Alneyadi & Normalini, 2023).

3.2.2 Regulatory and policy compliance

Cybersecurity is also influenced by regulatory compliance as a social factor. Studies indicate that while there are regulations on cybersecurity, compliance problems have contributed to inability of organizations to effectively fight cybersecurity threats (Wilner et al., 2021). The compliance problems include compliance being voluntary, bureaucracy, and employees choosing not comply with regulations and policies.
Voluntary compliance:

In some cases, compliance is voluntary. It means that people can choose whether to observe cybersecurity and this makes it hard to secure information systems against cyber-attacks as some people may choose not to observe the regulations (Badi & Nasaj, 2023). One of the key factors that contribute to voluntary is the organizational culture in relation to cybersecurity. If the organizational culture does not emphasize information security, then people may not feel obliged to take actions that are aimed to enhance cybersecurity (Yeng, Fauzi & Yang, 2021).

Bureaucracy:

There is also the issue of cybersecurity regulatory compliance being a hindrance to the development of good cybersecurity practices. Reviewed literature indicates that the compliance procedure in cybersecurity is long, bureaucratic, and tedious and as such, it makes it hard to effectively come up with ways of dealing with cybersecurity threats (Catota, Morgan & Sicker, 2019). Simply, regulatory compliance procedures in cybersecurity have become a threat to the best cybersecurity practices in organizations.

Employees choosing not comply with cybersecurity regulation:

Studies indicate that there are cases where employees in organizations choose not to comply with cybersecurity regulations and policies. One of the factors that contribute to this is compliance culture. Most organizations do not have a compliance culture (Marotta & Madnick, 2021). The lack of a compliance culture makes it hard for employees in organizations to take precautionary measures to prevent cyber-attacks. Employees in an organization may also decide not to comply with cybersecurity regulations because of intuitive cost-benefit analysis where one feels that the benefits that will be obtained for not following the company’s regulations and policies on cybersecurity outweigh the cost involved (Pollini et al., 2022). Simply, when individuals perceive the cybersecurity policies and regulations of their organization are too costly, they do not follow them.

Another key factor that contributes to non-compliance is workload. When employees have a large workload, their information security conscious behaviour reduces (Yeng, Fauzi & Yang, 2021). In other words, a large workload makes it harder for employees to focus on practices that are aimed to improve cybersecurity within their organizations (Yeng, Fauzi & Yang, 2021).
Poor compliance oversight and management:

Reviewed literature indicates that there regulators are less efficient in implementing the right oversight and management measures and this is due to not having knowledge of the new cybersecurity problems which have emerged (Marotta & Madnick, 2021). It implies that the compliance management measures regulators implement within organizations are effective when it comes to handling new cyber-threats and this contributes to cybersecurity problems (Marotta & Madnick, 2021).

Difficulty in implementing regulations:

Studies reviewed also suggest that most organizations have difficulty in implementing regulations and this is due to complexity of these regulations. The cybersecurity regulations are numerous and complex in nature (Marotta & Madnick, 2021). This has contributed to misalignment between organizations’ security goals and the regulations they are supposed to comply with (Marotta & Madnick, 2021).

3.3 Economic Factors

The reviewed literature suggests that the main economic factors influencing cybersecurity is financial constraints, budgeting, and misallocation of funds.

Financial constraints:

Smaller companies, for instance, do not have a budget for cybersecurity because it is too expensive (Kabanda, Tanner & Kent, 2018). These organizations do not have money to invest in cybersecurity systems and activities (Kabanda, Tanner & Kent, 2018). Reviewed literature shows that most organizations have limited resources and as such, cybersecurity is not a particular concern for them (Jalali & Kaiser, 2018). The limited resources means that most organizations are unable to employ specialists or create a cybersecurity department to deal with cybersecurity challenges (Mierzwa & Scott, 2017; Catota, Morgan & Sicker, 2018). The issue of resource availability is exacerbated by the fact that the cost of cybersecurity has been growing over time. Reviewed literature indicates that cyberattacks have increased and become more advanced over time and as a result, there is need to invest more in cybersecurity (Zhuo & Solak, 2014). This has put financial pressure on
organizations. It has also made it hard for organizations to effectively budget for cybersecurity.

**Budgeting:**

Budgeting is critical in the investment in cybersecurity as well as compliance with cybersecurity regulations as it ensures allocation of resources to these important areas (Marotta & Madnick, 2021). However, studies reviewed indicate that organizations struggle with budgeting due to rising cybersecurity and compliance costs (Marotta & Madnick, 2021). Organizations also suffer from budget restrictions that make it hard for them to allocate adequate resources to cybersecurity (Marotta & Madnick, 2021). Budget restrictions result in adoption of inadequate or unreliable cybersecurity measures (Marotta & Madnick, 2021). However, there are also cases of low budget priority with regard to cybersecurity (Kabanda, Tanner & Kent, 2018). It means that during budgeting, companies and institutions do not allocate adequate funds to cybersecurity even when there is financial capability (Catota, Morgan & Sicker, 2019). The limited budget prioritization of cybersecurity is due to limited support by the management. In some organizations, the management is not committed to cybersecurity and this contributes to limited prioritization of cybersecurity budget (Kabanda, Tanner & Kent, 2018).

**Misallocation of resources:**

Misallocation of resources emerges as a less prominent economic factor affecting cybersecurity. This is a situation where all resources are not allocated to serve a situation in the best way possible (Kianpour, Kowalski & Øverby, 2021). In relation to cybersecurity, it means that part of a firm’s operation is not given all the resources needed and this contributes to economic inefficiency (Kianpour, Kowalski & Øverby, 2021). In other words, misallocation of resources means that organizations have not managed to get the expected returns from cybersecurity.

**Investment in cybersecurity:**

Related to budget prioritization is the issue of investment in cybersecurity. Reviewed literature suggests that the ability to tackle cybersecurity problems depends on the level of investment in cybersecurity especially by private sector firms (Gordon, Loeb, Lucyshyn &
Zhou, 2015). However, studies also indicate that the level of investment in cybersecurity depend on incentives and regulations by government (Gordon, Loeb, Lucyshyn & Zhou, 2015). If the government provides incentives and enacts laws that promote cybersecurity investment, then private sector firms may be motivated to invest more in cybersecurity. Investment in cybersecurity is determined by resource availability. For example, the ability to acquire more sophisticated technologies, according to reviewed literature, is limited to organizations with larger budgets (Catota, Morgan & Sicker, 2018). In general, literature shows that more powerful firms have the financial capability to invest in cybersecurity which allows them to effectively deal with cybersecurity issues (Zhuo, Y., & Solak, S. (2014).

3.4 Environmental Factors

The main environmental factor as the reviewed literature is resource availability and resource constraints.

**Resource availability:**

While resource availability also falls under the economic factors, under environmental factors category, resource availability is considered from a broader perspective. For instance, the studies reviewed reveal that resource availability is not limited to financial resources (Kabanda, Tanner & Kent, 2018). It encompasses other resources such as technical resources. For instance, literature reviewed suggests that the management in most organizations do not have the technical know-how that would enable them to deal with cybersecurity problems (Wilner et al., 2021). In this case, the environmental factors are social nature as opposed to them being physical. In other words, cybersecurity is affected more by factors within the social environment as opposed to the physical environment.

**Resource constraints:**

Literature shows that most organizations have limited resources to invest in cyber-security (Kabanda, Tanner & Kent, 2018; Marotta & Madnick, 2021). However, most of the reviewed limit to the resource constraints to the financial resources (Kabanda, Tanner & Kent, 2018). Other resources such as the human resource and physical facilities are not addressed.

In the literature search, no sources could be found that examine the factors within the physical environment that could affect cybersecurity. These may include the built
environment, physical barriers, and even security infrastructure. For example, the built environment may be key to installation of cybersecurity systems. On the other hand, the physical barriers may make it hard for cybersecurity experts to access an area and install relevant systems. Such barriers may also make it hard to move equipment to an area. The question of the physical environmental factors affecting cybersecurity thereby presents a research gap that is supposed to be explored in future research.

3.5 Technological Factors

The reviewed literature suggests that the main technological factors influencing cybersecurity are evolving cybersecurity threats, availability of technology, new technologies and new cybersecurity measures.

Evolving cybersecurity threats:

A number of studies indicate that cybersecurity threats have evolved over time and this has made it hard for organizations and experts to effectively deal with the issue of cybersecurity (Nazah, Huda, Abawajy & Hassan, 2020; Alenezi, Alabdulrazzaq, Alshaher & Alkharang, 2020; Zimba, Wang & Chen, 2018). For instance, over time, more advanced malware have been developed. Literature indicates that initially, malware was not developed to cause damage. It was rather an experiment that went wrong and it led to emergence of malware. However, with the emergence of this initial unintended malware, individuals began developing malware with the intention of causing damage (Alenezi, Alabdulrazzaq, Alshaher & Alkharang, 2020). Literature also indicates that while initially, malware was developed by a few individuals, currently, governments are developing their own malware to spy on enemy countries or even cripple key infrastructure and systems (Alenezi, Alabdulrazzaq, Alshaher & Alkharang, 2020). Some of the most recent malware are Wannacry and NotPetya ransomware cryptoworms (Sapienza et al., 2018). Apart from the emergence of more sophisticated malware, different techniques have also been developed that can be used to attack network partitions and other systems (Zimba, Wang & Chen, 2018; Li & Liu, 2021). In general, new attack tools have been developed which are difficult to detect (Rajasekharaih, Dule & Sudarshan, 2020). This, coupled with the use of out-dated security tools and inadequate software, has increased cybersecurity risk (Rajasekharaih, Dule & Sudarshan, 2020).
Availability of technology:

The key to cybersecurity is technology that allows companies to effectively deal with cybersecurity threats. Some sources indicate that some organizations lack the technologies that can help them deal with these threats (Catota, Morgan & Sicker, 2018). Some of the contributing factors to the lack of technology are budget constraints and diversity of systems. Budget constraints, as studies reviewed, make it hard for organizations to acquire the necessary technologies that enable them to effectively prevent or handle security issues (Catota, Morgan & Sicker, 2018).

New technologies:

New technologies such as internet of things (IoT), big data, and blockchain have affected cybersecurity (Saeed et al., 2023). For example, the application of IoT has increased the exposure of the affected systems to cyber-threats (Lykou, Anagnostopoulou & Gritzalis, 2018). IoT also generates a lot of information and it is characterized by a high level of interconnectedness (Raimundo & Rosário, 2022). This has increased the vulnerability of systems to cyber-attacks. For example, cyberattacks can access the data and compromise it, causing systems to fail (Tschider, 2018). In general, IoT, as a technology, has a number of vulnerabilities that make IoT devices prone to cyberattacks. These vulnerabilities limited computational power, different devices involved in IoT having different architectures which makes it difficult to develop unified security framework, and limited user interaction which makes it hard to monitor potential cyberattacks (Mughal, 2019; Sha et al., 2018). However, these technologies, especially blockchain, have the potential of improving cybersecurity (Saeed et al., 2023) although even blockchain has also vulnerabilities that makes it prone to cyber-attacks (Abdelwahed, Ramadan & Hefny, 2020). For example, the key vulnerabilities of blockchain 3.0 which is the most advanced blockchain technology are attack against Hyperledger Fabric and the generals risk (Abdelwahed, Ramadan & Hefny, 2020).

Like IoT and blockchain, another emerging technology the smart technology which has also been used significantly (Mazhar et al., 2023). For example, it has been used to develop the smart grid (Mazhar et al., 2023). The challenge with smart technology is the same which is vulnerability to cyberattacks (Mazhar et al., 2023).

New technologies contribute to both increased level of cybersecurity vulnerability and capabilities (Raban & Hauptman, 2018). The key technologies which increase attack
capabilities and thereby cybersecurity vulnerability are internet of things (IoT), biohacking, and human machine interface (Raban & Hauptman, 2018). On the other hand, blockchain, artificial intelligence, and quantum computing are the technologies that have enhanced the defence capabilities (Raban & Hauptman, 2018).

**New cybersecurity measures:**

While new cyberthreats are developed daily, there are equally no security measures and systems that are constantly being developed to combat these threats. For example, Sapienza et al (2018), in their study, introduce the DISCOVER framework which is a method that uses text mining to generate warning of potential cyber-attacks. This method allows individuals and organizations to take measures to prevent attacks. Sources reviewed also indicate that there are also new detection methods which have been developed and which have reduced the impact of cyber-threats (Nazah, Huda, Abawajy & Hassan, 2020). They include tripwire, intrusion detection, and anomaly detection (Nazah, Huda, Abawajy & Hassan, 2020).

Other tools that developed which help to improve cybersecurity are Cyber-Ranges (CRs) and Test-Beds (TBs) (Ukwandu et al., 2020). These tools help to better understand the evolution of an attack and the appropriate method that can be used to counter the attack. Such methods have helped organizations to prevent cyber-attacks and protect their systems (Ukwandu et al., 2020). Apart from already developed methods, researchers are also suggesting strategies that can be used to promote cyber-security. For example, Ali et al (2023) propose system architecture for shielding secrets in cyber-physical systems. The architecture comprises of cyber-physical systems, consortium blockchain, secret management, and privacy-enhancing techniques among many other components. Prasad and Rekha (2023), on their part, propose a blockchain-based IAS protocol which incorporates access control, secure, and identity authentication to enhance security of cloud computing. Chentouf and Bouchkaren (2023) also point to the significance of blockchain as a technology that can be used to enhance cybersecurity. The key characteristics of blockchain that makes it ideal as a solution to cybersecurity are pseudonymity, decentralization, security, and immutability.
4 Comprehensive Framework

Insights obtained from the systematic literature review were critical in the development of the comprehensive framework for influential factors in industrial cybersecurity. The comprehensive framework consists of four main factors which are social, economic, environmental, and technological. As highlighted, these factors influence cybersecurity, by either limiting or promoting it. Under social factors there are two main sub-factors which are human-related factors and regulatory and policy compliance factors. The human-related factors have emerged as the main influence on cybersecurity. For example, lack of knowledge and skills, poor attitude towards cybersecurity, and negligence have contributed to poor cybersecurity. These human factors have also contributed to low compliance level although other regulatory compliance factors like difficulty in implementing regulations have also contributed to poor cybersecurity situations in many organizations.

The key economic factors, as discussed above, are resource constraints, budgeting, misallocation of resources, and investment in cybersecurity. It was determined that many organizations do not have adequate resources and has limited the investment in cybersecurity. Resource constraints have led to budgeting problems with budget prioritization in relation to cybersecurity low. Two main technological factors influence cybersecurity and these are new technologies and new cyber threats. New technologies have exacerbated the cybersecurity problems in some cases and improved defence capabilities in other cases. The figure below shows the comprehensive framework.
Fig 4: Comprehensive framework for Industrial Cybersecurity and its factors explored in existing literature
5 Research gaps and future research directions

An examination of the literature reviewed in this study reveals a number of research gaps that need to be addressed.

5.1 Lack of research on Physical environment

The main one is in relation to environmental factors. The reviewed studies focus on the social and organizational environments but fail to pay attention to the physical environment and how it influences cyber-security (Singh & Singh, 2022). The physical environment can play a role in cyber-security. For example, the built environment is critical security as it determines the availability of facilities that allows for installation of security systems (Marotta & Madnick, 2021). A critical element in cyber-security is the internet. It implies that if a region does have internet connectivity, the level of cyber-security is affected. However, the studies reviewed fail to examine such aspects of the physical environment that may influence cyber-security.

5.2 Solutions to emerging cyber-threats

Another research gap is an examination the key solutions to emerging to cyber threats (Nazah, Huda, Abawajy & Hassan, 2020). While the studies have highlighted new cyber-security measures that have been developed over time, there was study that addressed specific cyber-threats. For instance, one of the studies pointed to emergence of Wannacry as a new form of ransomware that is being used to attack systems (Sapienza et al., 2018). However, it did not highlight whether security experts have developed a countermeasure to deal with this threat.

5.3 Limited empirical evidence

Lastly, there is a research gap in relation to empirical evidence to support the level of industrial cyber-security. A few studies have provided such evidence but it is limited. For
example, one study has highlighted the number of emails that have been hacked in an organization (Ani, He & Tiwari, 2019). However, there is limited evidence that shows the extent of the cyber-security problem and the main factors that have contributed to the problem (Catota, Morgan & Sicker, 2018). For instance, while it has been acknowledged that human factors are the main determinant of cybersecurity issues experienced in many organizations, the studies reviewed provided limited evidence that directly links these human factors to cyber-security issues experienced.

The above research gaps imply that there is need for further research on industrial cyber-security to gain better insight into the problem and how to resolve it. For example, an examination of each emerging cyber-threats and its corresponding counter-measure will reveal the threats that have not been addressed and how this influence cyber-security.
6 Discussion

6.1 Key findings

The main goal of this study was to examine the influential factors in industrial cyber-security. The more specific objectives were examine the social, economic, technological, and environmental factors influencing cyber-security practices and the implication of incorporating emerging technologies in cyber-security. To address the above objectives

On the question of social factors, the systematic literature review carried out indicated that human-related factors are the main social factors influencing cyber-security. Some of these human-related factors are knowledge and skills, negligence, attitude, malicious intent, human behaviour, education, and resistance to change. For instance, it was established that most people do not have knowledge of cyber-security and the skills to handle cyber-security problems (Ani, He & Tiwari, 2019; Singh & Singh, 2022; Pollini et al., 2022). Other people are not aware about cyber-security and as such they are unable to detect any cyber-attacks and thereby take appropriate action.

The reviewed literature also revealed that there is a tendency of people to be negligent. Most people, even those who are aware of cyber-security threats, do not act in the manner that protects their systems against potential attacks. For instance, most people do not review their passwords constantly (Yeo & Banfield, 2022). People are also not keen on the actions they take daily when using systems and handling information. There are cases of people misplacing hard drives even when they hold sensitive information. This increases the risk of such hard drives falling into wrong hands.

The attitude towards cyber-security, based on reviewed literature, is dismissive. Most people do not pay particular attention to cyber-security and only act when they experience actual attacks. The dismissive attitude towards cyber-security is possibly due to the feeling that cyber-security is not a significant threat and that even if it occurs, it is impact is minimal (Yeng, Fauzi & Yang, 2021). Some individuals feel that their organizations do not have the technologies that make them vulnerable to cyber-security and as such, they do not feel the need to take any proactive measures to prevent potential cyber-attacks.
While most cyber-security incidents are a consequence of negligence, reviewed literature also shows that there are cases where individuals deliberately engage in activities aimed at harming their organization’s systems (Yeo & Banfield, 2022; Wilner et al., 2021). This is normally the case among disgruntled employees who feel that they have not been treated fairly.

The key factor that determines knowledge and skills is education. However, systematic literature review in this case shows that the existing education is not in line with cyber-security needs, meaning that the knowledge and skills acquired by those who take courses in cyber-security are not adequate the prevailing cyber-security challenges (Catota, Morgan & Sicker, 2019). With regard to human behaviour, it was established in this study that people’s behaviour towards cyber-security is careless and risky. Cyber-security has not been given priority by most people, even those in organizations’ leadership. Lastly, it was found that some people are resistant to change and this includes any attempt to implement cyber-security measures (Catota, Morgan & Sicker, 2019). The resistance to change is as a result of the fear of losing their jobs.

With respect to regulatory and policy compliance as a social factor, systematic literature showed that there is limited compliance with the regulations and policies which guide cyber-security activities. This is due to compliance being optional in some cases and people simply choosing not to comply with these regulations (Badi & Nasaj, 2023). However, there are cases where the cyber-security regulations and policies are complex and many, making it hard to observe and implement all of them.

The economic factors identified from the systematic literature review are financial constraints, budgeting, misallocation of resources, and investment in cyber-security. It was established that many organizations do not have adequate financial resources to effectively invest in cyber-security (Kabanda, Tanner & Kent, 2018). However, there are cases where cyber-security is not prioritized during budgeting. In other words, inadequate funds are allocated to cyber-security, with companies focusing on other seemingly more important operational aspects.

In relation to misallocation of resources, reviewed literature suggests that there are cases where while funds have been allocated to cyber-security, the aspects emphasized on in the allocation are those which cannot effectively address the cyber-security issues faced
(Kianpour, Kowalski & Øverby, 2021). Ultimately, even with adequate resources, cybersecurity problems are likely to persist. Lastly, literature reviewed suggests that there is limited investment in cyber-security and this is because resource availability challenges.

With respect to technological factors, it was found in this study that the key factors are new cyber-threats, availability of technology, new technologies, and new cybersecurity measures. New more sophisticated cyber-threats have been developed and this has increased the cyber-security risk (Alenezi, Alabdulrazzaq, Alshaher & Alkharang, 2020). Literature review also shows that some organizations do not have the necessary technologies to deal with cyber-security threats. On the other hand, it was found that new technologies such as AI, IoT and blockchain have increased to vulnerability of information systems to cyber-attacks in some cases but also helped to improve the defence capabilities of these systems when used to appropriately (Catota, Morgan & Sicker, 2018). Lastly, it was established from the systematic literature review new cyber-security measures have been developed to counter existing threats. In general, it was found that technology has increased the cybersecurity vulnerability of systems but also improved their defence ability against cyber-attacks.

Lastly, on the question of environmental factors, it was established that limited research has been carried out in this area, especially in relation to the factors within the physical environment. The only environmental factor identified is resource availability (Wilner et al., 2021). This factor was considered from a broader perspective beyond financial resources.

### 6.2 Practical Implications

One of the practical implications of the findings from this study is companies need to invest in training of employees in relation to cyber-security. As established, few people have knowledge and skills to deal with cyber-security problems faced by their organizations (Singh & Singh, 2022). Business organizations thereby need to invest in training to equip their staff with necessary knowledge and skills that would enable them to identify and deal with cyber-threats.

The results also imply that business organizations should develop a cyber-security culture in their operations. From the findings, it can be deduced that there is limited focus in cybersecurity in most organizations as reflected in negligent behaviour among employees and
limited budget prioritization (Yeo & Banfield, 2022). A cyber-security culture will see people reduce engaging in risky behaviour such as opening emails from unknown sources, misplacing hard drives with sensitive information, and maintaining the same predictable passwords for long.

The results obtained also imply that there the government should streamline the regulations on cyber-security to make it easier for individuals and organizations to comply with these regulations (Marotta & Madnick, 2021). As established, one of the compliance challenges faced by business organizations is having numerous and complex cyber-security regulations (Badi & Nasaj, 2023). Streamlining these regulations by collapsing them into a few simple and straightforward regulations will enable organizations to determine the course of action to take to improve their cybersecurity while still observing the necessary laws and regulations.

Other practical implications include the government should provide incentives to businesses in relation to cyber-security and there is need to develop more sophisticated cyber-security countermeasures. One of the challenges faced by organizations is financial constraints in the face of increasing cost of cyber-security (Mierzwa & Scott, 2017). Governments should support businesses to invest in cyber-security. On the other hand, businesses should invest in the development of more cyber-security measures in order for them to effectively deal with emerging cyber-threats.

6.3 Research Implications

As demonstrated, there are various areas which have not been handled effectively in existing studies. It thereby implies there is need for more research to on cyber-security. One area future research should focus on is environmental factors affecting cyber-security. The idea is to determine if the built environment affects cyber-security. The results obtained also point to limited empirical evidence about cyber-security incidents and the influencing factors. Future research should thereby focus gaining more knowledge about cyber-security, the main challenges, and the influencing factors. This will help determine the course of action that should be taken to improve the level of cyber-security.
7 Conclusion

The aim of this research was to examine the influential factors in industrial cybersecurity. In particular, the focus was to determine the social, economic, technological, and environmental factors affecting cyber-security. Data was collected using systematic literature review. The search for sources was done in two databases which are Scopus and Web of Science (WOS). The search produced 40 relevant sources which were reviewed and valuable information extracted.

The findings obtained were arranged under the four factors highlighted above. The main social factors identified from the reviewed literature are human-related factors and regulatory and policy compliance. The human-related factors include knowledge and skills, negligence attitude, risky behaviour, and education. It was found the level of cyber-security knowledge and skills among people is low and this reduced the ability of individuals and organizations to address cyber-security challenges. On the other hand, people are generally negligent when handling sensitive information and key systems and this puts them at a risk of being attacked. People are also constantly engaging in risky behaviours such as misplacing hard drives, sending emails without confirming the validity of the recipient, and not updating passwords regularly. Lastly the current education on cyber-security is inadequate meaning that knowledge and skills acquired cannot help to effectively deal with cyber-threats.

Economically, it was found the main factors include financial constraints, budgeting, and misallocation of resources among others. Most organizations do not have adequate financial resources to invest in cyber-security. Other organizations, while they have resources, do not prioritize cyber-security in their budgeting process. There are also cases where there is misallocation of resources, meaning that resources are not used to effectively address cyber-security problems.

The technological factors identified from the systematic literature review are new technologies, new cyber-threats, and availability of technology. New technologies like artificial intelligence, blockchain, and internet of things (IoT) have had a significant impact on cyber-security. These technologies have made information systems to be more vulnerable to cyber-attacks although some of them like blockchain and quantum computing have
enhanced the defence capabilities of these systems. New malware have also been developed, increasing the cyber-threat. Lastly, some companies do not have access to technologies that can help them deal with cyber-threats effectively.

The reviewed literature did not address the question of environmental factors in detail, especially if one is considering the physical environmental factors. However, the studies focus on the organizational environment, with resource availability being the main factor influencing cyber-security in this environment. The results imply that organizations need to invest more in training their employees in cyber-security, improve their cyber-security budgeting, and invest in better cyber-security technologies. This will help them handle cyber-threats better.

7.1 Limitations

While this study provides insights into the cyber-security and the influencing factors, it has also a number of limitations. One of them is an overreliance on secondary sources. The results in this study are obtained from existing studies. It means that mistakes committed in these reviewed studies are propagated in this study. For example, it is possible that some researchers were biased in their studies or simply made mistakes when collecting and analysing data. If such mistakes were committed, then it means that they have been carried over into this study.

Another limitation is the search for sources was limited to two databases. The two databases used in this study are Scopus and Web of Science. However, other databases have valuable sources. For example, Google Scholar is one of the databases that have sources covering a wide range of subjects. Overlooking these other databases may have led to missing out on more relevant sources that could have provided better insight into the influential factors in cybersecurity and improved the accuracy of the results obtained.

Lastly, the study does not contribute any new knowledge on industrial cyber-security. As pointed out, there are aspects such as environmental factors that existing literature fails to address. These issues remain unaddressed in this study since it relies on the same existing literature. As such, while the study brings together information from various sources, making
it possible to determine what has been studied about cyber-security, it does not add value to existing knowledge.
References


