KASBIT BUSINESS JOURNAL

Journal homepage: www.kbj.kasbit.edu.pk

Developing cyber security strategies for business organization to prevent data breaches

Basheer Ullah[i*], Syed Irfan Nabi[i]

i) Department of Computer Science, School of Mathematics and Computer Science, Institute of Business Administration, Karachi

ARTICLE INFO

Keywords:
Criminal activity, Cybercrime, Small businesses, Data breaches, Cyber security strategies, Grounded ontology methodology

ABSTRACT

One of the crucial and fastest growing areas of criminal activity is cybercrime. Most of the small businesses do not have the financial and technological means to protect their systems from cyber-attacks, leaving them vulnerable to data breaches. This study aims to explore this issue using case study method based on examination of cyber security strategies employed at small business. Primary data is collected through an on-line survey from (50 business companies) and semi-structured interviews. Using the first stage of grounded ontology methodology, the result show that the small businesses should utilize the managed cybersecurity services offered by experts as an outsourced service and that cybersecurity awareness among the users must be diligently promoted since the humans are the weakest link. These recommendations should be useful for the small businesses.

Introduction

Cyber security breaches have been gaining prominence in the news highlights as the world is opening up the space for hackers to breach the cyber security by adopting online systems and services (Behera et al. 2022; Parkinson and Khana 2022). The last two years of lockdown and social distancing (Khan et al. 2020; Pranggono and Arabo 2021; Lallie et al. 2021) has seen many news small businesses crop up in the online arena while various existing businesses had to move online as well. The Internet has provided small businesses with an opportunity to compete in a global market, making Small businesses are highly dependent (Ghobakhloo and Tang 2013). Multiple types of public and private sector businesses have been able to manage their companies via online electronic data connections (Bernik 2014). However, it has exposed these businesses to cyber-attacks and data theft. Although persistent threat of cyber-attacks exits, yet, the small business employees can be confident that their technology is secure because they receive no notifications of attacks or threats, which is why many small business attacks go undetected (Harsch et al. 2014). Many small businesses lack awareness and knowledge of the threats posed by cyber-attacks Small business owners struggle to keep their company and customer data safe and secure from external threats (Goode et al. 2017). To secure their

Corresponding Authors:
[*] Email: b.ullah.23238@khi.iba.edu.pk (Basheer Ullah)

Received 7, Dec 2022;
Received in revised form 31, Dec 2022
Accepted 25, Dec 2022

The material presented by the authors does not necessarily represent the viewpoint of the editor(s) and the management of the Khadim Ali Shah Bukhari Institute of Technology (KASBIT) as well as the authors’ institute.

© KBJ is published by the Khadim Ali Shah Bukhari Institute of Technology (KASBIT) 84-B, S.M.C.H.S, off Sharah-e-Faisal, Karachi-74400, Pakistan

upon technology to do business and keep data.

small business owners lack effective cyber security strategies. While it has expanded business opportunities, especially for the small businesses, at the same time it has increased the vulnerability of the system to targets by criminals/hackers. Due to lack of resources as the businesses are being small, they do not focus the cyber security threats. The sensitive business information combined with other data is made available as a high prized digital assets (Günther et al. 2022; Glas 2022; Su 2020) by the businesses going online. This has become a lucrative target of the cyber criminals. Therefore, the digital assets and the infrastructure needs to be safeguarded.

It is observed that small business face cybersecurity challenges and are neither properly equipped to defend against them nor sufficiently aware of the threats posed by being connected to the Internet. The aim of this research is to add knowledge to fill the gap in business practice related to cyber security policies in small businesses. Small business, who lack adequate cyber security strategies to protect information systems from cyber threats could benefit from this study. The survey followed-up by interview of executives from small businesses shall help understand the research problem.

With more data being made available online due to operational needs of businesses any data breach is highly publicized by media since its impact has increased over years. Phishing emails and ransom ware have become a detrimental to the existence of small businesses. Generally the small businesses do not have effective and adequate technical cybersecurity measures in place (Yee and Zolkipli 2021; Firmansyah et al. 2020). Further, the central actor in these cases is the human. Thus, human factors have to be taken into account as well. This is not limited to small businesses rather a variety of industries and companies have been victims of cyber-attacks. No one is safe. Retail, banks, hospitality, medical and social media, to name a few, have been targeted in recent times.

As one of the most common attack vectors is the insider. About 20 % of small businesses rely on their security department to defend against internal attacks, compared to 62 percent of larger businesses. The common business problem is that many security resources in small businesses are scarce or unavailable (Wang and Johnson 2018; Wang and Park 2017). According to (Ter 2018) the threat of cyber-attacks on global companies is increasing as

business and customer data from cyber-attacks,

more companies become target for commercial secrets, sensitive business data and customer information. The costs of data breaches for global companies rose from $850,000 in 2014 to $1.3 billion in 2016 and has created a global cybersecurity market of $170.4 billion in 2021 (Kim et al. 2018). A common business problem is that data breaches may damage the reputation of the company's brand and lose customers' confidence. The significant issue is that some small business owners lack cyber defense strategies to protect business data from cyber-attacks (Ter 2018).

Thus, it can be seen that small business face cybersecurity challenges and are neither properly equipped to defend against them nor sufficiently aware of the threats posed by being connected to the Internet.

This is exploratory research, with the aim to gain insight and find out the sort of cybersecurity measures and strategies are used by the small businesses and to recommend industry best practices for them. This study aims to answer the below questions in systematic which are supported by the empirical evidences.

- What existing cybersecurity strategies do leaders of small businesses use to protect their systems from cyber threats?

- What cybersecurity strategies will leaders of small businesses implement to protect their systems from data breaches?

The aim is to add knowledge to fill the gap in business practice related to cyber security policies in small businesses. Small business, who lack adequate cyber security strategies to protect information systems from cyber threats could benefit from this study. The survey followed-up by interview of executives from small businesses shall help understand the research problem

The remainder of the paper is organized as follows. Section 2 highlights the relevant literature. Methodology, research design and data collection method are discussed in section 3, while section 4 presents the main results and recommendations. Lastly, conclusion is given in section 5.

2. Literature Review

The rapid digitalization and increased connectivity of the Internet have led to the increase in c ' x threats to the security of the Internet. The ir 63 t cyber security threats on a massive global scale have prompted countries to review and strengthen their national cyber security strategies and enact new and bolder legislation that is both comprehensive and far-reaching (Kosseff 2020; Christensen and Liebetrau 2019).

According to U.N. International Telecommunications Union (ITU) survey Singapore is the world’s most connected country to the world and its cyber security strategies are ranked among the world’s top strategies (Tehrani et al. 2013; Hamilton et al. 2002; Myftari 2021). Therefore, we consider it as role model at length and compare the adopted strategies by the small businesses. Based on the legal, technical, organizational institutions, educational and research capacity of Singapore and cooperation in the information sharing network Since 2003, the agency has been preparing a high-level national cyber security strategy and a high-level national cyber security plan (Senol and Karacuha 2020; Ron et al. 2020; Shafqat and Masood 2016).

Consequently, Singapore’s strategy involves multi-pronged participation (Allam 2020) of experts, public, private and public sectors. For example, efforts are being made to raise awareness of information technology security and adopt security measures in companies and users through online and social media platform advertising program, conferences, educational talks, roadshow and printed advertisements. (Ter 2018; Allam 2019; Pauletto 2020)The need to increase the pool of information communications security in Singapore, due to a shortage of local cyber security professionals, experts will work together with higher education institutions to integrate cyber security into the curriculum, and to implement specialized courses in the current programme, to address the problem (Gorian 2020).

According to Li and Liu (2021) currently, most of the countries’ economic, trade, cultural, social, and intergovernmental activities, including individuals and non-governmental organizations, are active at all levels and government institutions operate in cyberspace. In recent years, many private and government organizations around the world have been confronted with the danger of cyber-attacks (Alazab et al. 2021; Wan et al. 2021) and wireless communication technology. Today’s world relies heavily on electronic technologies, and protecting these data from cyber-attacks is a complex problem. The aim of cyber-attacks is to cause financial harm to companies. In other cases, cyber-attacks may be used for military or political purposes. To this end, various organizations use different solutions to prevent cyber-attack damage. Cyber security follows the latest information in real time on IT data. Scientists around the world have so far proposed several methods to prevent or reduce cyber-attacks (Eling et al. 2022; Akintoye et al. 2022).

National Cyber Security Strategy (NCSS) of EU covers the prevention perspective from the beginning to the end. According to Senol and Karacuha (2020) NCSS with the aim of effectively counteracting and ensuring cyber security, studies are being carried out in all countries into which paths should be taken and which methods should be used to develop, create and implement an NCSS. In this context, by explaining the importance of cyber power, the need to consider cyber power as one of the elements of national power (Osho and Onoja 2015; Kamin 2017; Rajan et al. 2021) and the importance of providing security against cyber-attacks with cyber power deterrence are discussed while a proposed a new and integrated approach (H. A. M. Luiijf et al. 2011; E. Luiijf et al. 2013; Izycki and Colli 2019; Zimmermann and Renaud 2019) to the creation and implementation of an NCSS and an authoritarian organizational structure responsible for this strategy. It can be concluded that the proposed effective and deterrent NCSS model and approaches could help to handle these issues efficiently and effectively to better manage, control and audit cyber security issues (Benoliel 2014; Shackelford 2019; Cristiano 2021). Providing new concepts on cyber security issues, supported by cyber power and deterrence on this issue in the world; Adoption of an integrated approach to cyber security strategies and policies in the development and implementation phases of an NCSS; bring in a range of topics in support of cyber security and defense from different perspectives; and achieve a high degree of success with the proposed approach, particularly in terms of effectiveness and the existing basic structure deterrence strategies and action plans (Brangetto and Aubyn 2015; Sayin and Başar 2017; Liveri et al. 2018; Żywio\lek et al. 2021).

Regarding cyber security as a matter of national security, Taiwanese authorities passed the Information and Communication Management Act (ICM Act) in May 2018 in response to increasing awareness of potential malicious cyber-attacks on the public and private sectors (Huang 2020; Ademola

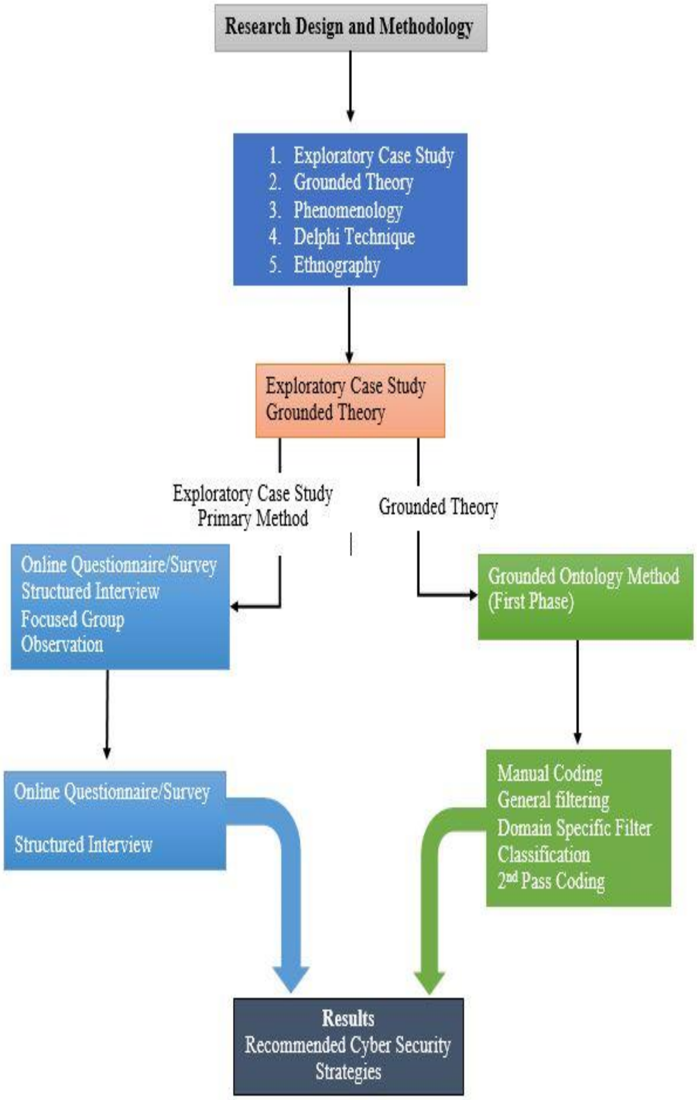
2022). Hsini Huang and Li (2018) have stated that according to the ICM Act, both governmental and non-governmental bodies must comply with the codified regulations and the new management scheme. The new basic law for cyber security requires all government agencies and operators of critical infrastructure (Hou et al. 2020; Michalec et al. 2020) to comply with the new regulation. In addition to the legal basis, state policy adopts traditional policy tools as economic stimulus, such as announcing a series of national development programs, introducing new safety standards, and providing financial subsidies and R&D loans to SMEs (Nanto 2009; Song and Zhou 2020; Alber 2020).

Goel (2020), Deora and Chudasama (2021) is of the opinion that countries are exploiting the social and economic advantages of the Internet and are afraid of threats to national security. In response to these threats, countries are gradually strengthening their Internet borders and developing cyber weapons to prevent and mitigate conflicts. A potential downside of such federal regulation is inhibiting the rapid innovation that the Internet has traditionally fostered and restricting freedom of expression that has led to social inclusion in society (Goel 2020; Deora and Chudasama 2021).

On securing sensitive information and source of latest information on cybersecurity (Nifakos et al. 2021; Dalal et al. 2022; AL-Nuaimi 2022) argue that many companies own sensitive customer information (such as medical records, educational records, payment card details, personally identifiable information, and purchase patterns) as well as corporate intellectual property. Although cyber security is an issue that affects virtually all organizations and their employees, the overwhelming majority of published research cyber security currently does not come from articles in peer-reviewed organizational science journals, but rather from mass media articles, company technical reports, and peer-reviewed Journal articles from the disciplines of computer science, business informatics and information technology (Nifakos et al. 2021; Dalal et al. 2022; AL-Nuaimi 2022).

According to Al-Ghamdi (2021) cyber security is a complex challenge that includes several different aspects of governance, policy, operation, technology and law. The guide attempts to identify, organize and prioritize many of these areas on the basis of existing models, frameworks and other well-known references. The study focuses on protecting civilian aspects of cyberspace and therefore highlights the overarching principles and best practices that need to be considered when formulating, developing and managing a national cyber security strategy (Al-Ghamdi 2021).

While Idahosa (2020) and Aurelien (2021) warns that small business owners who fail to effectively protect their business data are at high risk of a cyber-attack. The numbers of data breaches against small businesses have increased, this has become a growing concern for consumers who rely on small business owners to protect their data from data breaches (Idahosa 2020; Aurelien 2021).



3. Research Design and Methodology

3.1. Research Design

There are various classes of qualitative research design; exploratory case study, grounded theory, phenomenology, the Delphi technique, ethnography and case studies, which can be adopted to come up with an appropriate answer to the posed research question. However, we are employing the exploratory case study design with grounded theory as it seems more relevant and suitable to evaluate the small businesses leaders' responses to an event of data breach. To look at the practices and experiences of small business entrepreneurs and their cyber security strategies, there would not be a single set of outcomes or responses, rather there would be multiple ways that can be adopted to prevent the cyber data breach, and hence, the exploratory case study and grounded theory seems more relevant in this real-world to deal with multiple aspects of the enquiry.

Exploratory case study's objective is to search key solutions and answers to the questions of 'what' or 'who'. Furthermore, exploratory case study data collection procedure is usually joined with the additional data collection procedure(s) like questionnaires and interviews, which helps to answer the research questions more precisely and clearly. In this research it is used with interpretive paradigm and grounded theory approach to find answers to the questions such as what, why and how.

Exploratory research is often described as method used to find out a problem that is not properly described previously and is often executed when the problem is at initial stage. It is conducted to have a finer understanding of the existing issues. A vital importance is that the researcher must be willing to modify his/her thoughts or orientation, subject to the disclosure of new data or revelation about the topic. Moreover, in Grounded theory framework, the objective is to understand the social world through theoretical sampling and estimations through datasets and come up with some new evidences regarding some theory.

Here the objective is to examine the internet security practices, and to explore effectiveness of the current strategies to prevent the cybercrime and come upwith recommendations for improving them. Therefore, the exploratory research methods seem more suitable that will be helpful to discuss the issue more in depth and come up with more solid and empirically evident conclusion and recommendations.

The given diagram highlighted the sketch of Research Design and Methodology section

3.2 Methodology

As the objective is to figure out the techniques of cyber security that helps the small businesses to enhance the system security and protect against the data breach, the qualitative exploratory research framework is used to find out the most popular cyber security techniques for the small businesses to provide the security against the data theft and breaches. In qualitative research the analysis and interpretation are done in conjunction with data collection. In Grounded theory, a novel theory/ idea is brought to the surface regarding a specific phenomenon after a thorough investigation of the relevant collected. The collection of iterative data and examination happens till theoretical saturation is reached after which additional data did not provide any further insight (Glaser and Strauss 2017). Grounded theory consists of four phases:

In the first phase includes notions taken from interviews, observation, and reflection. The second phase includes organization of the data into various groups which manifest the representation of themes. In the third phase, groups are formed and compared with one another, and consequently two or more competing theories are identified. The fourth and the final phase includes the development of the research hypothesis statement or concept map.

Here, we used the exploratory case study and grounded theory because it seems more suitable and appropriate for understanding and evaluating the small businesses point of view and their plans for the cyber security against data breach. This approach enables us to come up with clearer comprehension of the individuals' perceptions, believes, and experiences. The grounded theory is used for extracting meaningful themes with the objective to understand the social world through sampling and estimations from the participants' responses corpus. Following Percy, Kostere, and Kostere (2015) in this research the primary themes are extracted and evaluated from each online filled questionnaire. By extracting and synthesizing the primary themes from the collected data, we are able to create a category code list. Clear trends appeared when all the data from all the people is pooled.

The initial responses are collected from the participant through an online questionnaire with both closed and open-ended questions. Exploration of the data from each online questionnaire allowed us to construct the overarching themes to develop a categorical code database. A combination of the data from all participants revealed consistent patterns. Synthesizing the topics provided a full picture of the data collected regarding the research question.

3.3. Survey and Data Collection

To thoroughly investigate the issue, we have used two distinct methods for data collection. First, a self-managed questionnaire is used to collect the data from the small businesses. Second, semi structure interviews are conducted of the respondents of questionnaire in order to understand their point of view in more detail and precise way and avoid confusion in the responses.

Since, an email survey was chosen as the major data collection method as an email-based surveys are often the cheapest choice. An email was used as means of communicating with respondents and Google forms was used to capture responses of the respondents. The survey involved contact with business organizations and email out to the domain experts. In the first cycle the questionnaire was mailed to known expert for collecting data, later numbers of different small business organization experts were contacted for the purpose of data collection. Only some of them participated in the survey.

In the second stage, a qualitative semi-structured interviews of selected respondents were conducted in order to collect "better" data through the direct interaction with them. This interaction was helpful to enable the respondents to answer survey questions in an objective manner. The interviews involve both planned and unplanned questions. Five small company were targeted to collect data. Thematic coding using grounded ontology method Nabi (2013) of the online questionnaire replies served as the foundation for a codebook. To reach the saturation point, two participants are interviewed in semi-structured way to obtain more information and data.

4. Results, Data Analysis, and Interpretation

This section consists of three subsections. In the first stage we are using the Grounded Ontology (GO) method which consists of five steps, to extract the key words and its reference. In the second sub-section these key words are analyzed to extract the generalized and derived understanding. In the third sub-section the results saturation is discussed.

4.1. Grounded Ontology (GO)-Coding

We use the multi-step, multi-stage Grounded Ontology (GO) method developed by Nabi (2013) for obtaining understanding from the collected responses and a get a sense of what is being done and why in our target organizations. The GO method is a comprehensive methodology for developing ontology. However, our research was limited to extraction of major themes and their response we use only the first stage - the Coding stage - of GO methodology. Among the four stages discussed by Nabi (2013) only the coding stage is used in our case employing all of its five steps. The Coding steps is given in figure 1. Different coding techniques are used in each step. In the first step manual coding is done where all possible nouns and phrasal nouns and noun phrases are extracted from the text. This list is labelled Manual Coding. In the second step of ‘General Filtering’ we removed the non-related nouns/phrases from the list and is labelled as General Filtering. The third step is ‘Domain specific filtering’ where nouns/phrases not related to the topic are excluded. The fourth step involve the extraction of all the relevant words are sorted into various categories. In step five, the confirmed list of the categorized entities is retrieved in order to analyze the entities, their classification and affiliations between them.

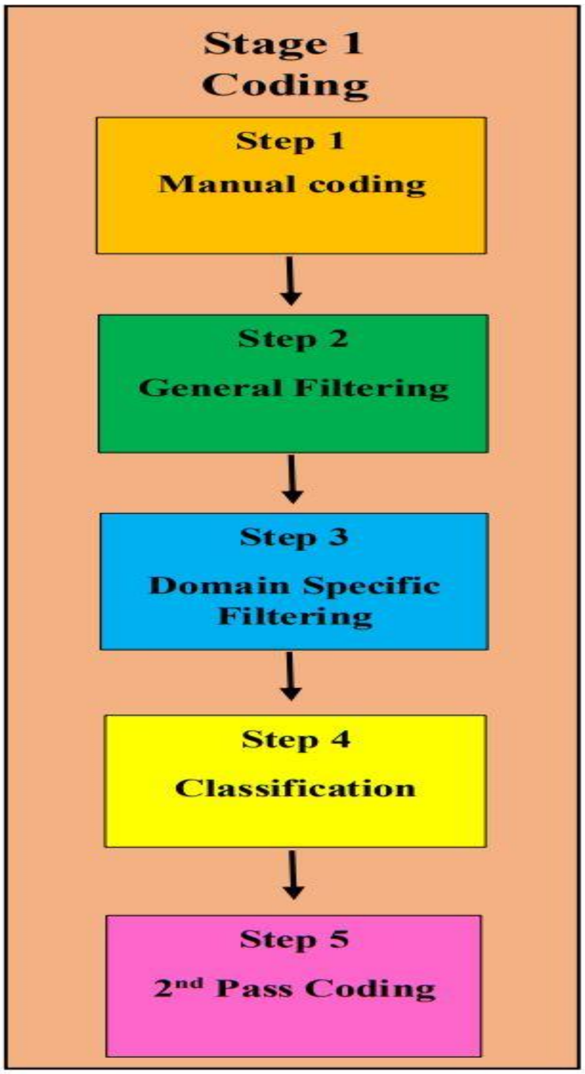


Figure 1: Stage-1 of GO-Methodolody, the Coding stage and its five steps

In the manual coding step, nouns and noun phrases were manually sorted from the collected data. Later, it was arranged alphabetically. Furthermore, the screen shot of the sorted nouns and noun phrase is shown in the table 1.

Table 1: Nouns, Noun Phrases & Alphabetically Order

Nouns and Noun Phrases	**Alphabetically Order**
Internet	Access
Https	Antivirus
Interceptions	Assets
Interruptions	Attacker
Content	Authentication
Connection	Business
SSL Certificate	Body
Hackers	Categories
Place	Communications
Network Firewall	Companies
Network Traffic	Computer Equipment
System	Connection
Website Protection	Containment
Employ Penetration	Content
SIEM System	Credentials

We also tried the mixed method research method as according to Leedy and Ormrod (2015) it provides a thematic conclusion and more comprehensive answer to the posed questions (Leedy and Ormrod 2015). The survey instrument includes closed-ended items but not much treatment has been done to the results obtained from them as the quantitative analysis does not fit research questions posed. The objective is to investigate responses of small businesses with reference to their cyber security measures for protection against the data breaches. Though it would be more comprehensive as it combines both qualitative and quantitative methods frameworks, yet does not seem relevant for this research.

We have also tried automated tool NVivo for coding to extract meaningful terms and phrases from a corpus, but it seems that in the case of NVivo coding is not capturing the real sense of the answers.

In second step which is general filtering, all the collected data was filtered generally, irrelevant words were eliminated from the data, to illustrate, body and content. The data has shown in table 2.

Table 2: General Filtering

Access	Access
Antivirus	Antivirus
Assets	Assets
Attacker	Attack
Authentication	Authentication
Business	Business
Body	Body
Categories	Categories
Communications	Communications
Companies	Companies
Computer Equipment	
Connection	
Containment	
Content	
Credentials	Credentials

At the Domain Specific-Filtering step, the nouns and noun phrases sorted from the collected data were eliminated which are not related to the specific domain, for instance, revenue and structure. The data has shown in the table 3.

Table 3: Domain Specific-Filtering

Access	Access
Antivirus	Antivirus
Assets	Assets
Attack	Attack
Authentication	Authentication
Business	Business
Body	
Categories	
Communications	Communications
Companies	Companies
Credentials	Credentials
Customers	
Cyber Security	Cyber Security
Cybercriminals	Cybercriminals
Cybersecurity Awareness	Cybersecurity Awareness

In the Classification step, all the relevant words were having relationships were sorted into various categories, to illustrate, access which included communication, restrict user access, wireless access point. The data has shown in table 4.

Table 4: Classification

Access	Access Communication Restrict User Access Wireless Access Point	
Assets	Assets Companies Employee Organization Data Software	Business Industry
Attacks	Attack Cyber Security Breaches DDoS Attack Malware Phishing Spyware SQL Injection Worms	Cybercriminals Ransomeware

In the last step, which is the second pass coding, the confirmed list of the categorized entities list has shown in the table 5.

While in the second pass coding, i.e., security is a part of security measures so they are placed in one category by the name security measures. Another example is that Threats and Theft are placed in one category by giving them a name as threats. Hence, it illustrates that Go |methodology is used to analyze the entities, their classification and affiliations between them

. ***Table 5: 2nd Pass Coding***

Access	
Assets	
Attacks	Attacks
Threats	
Security Measures	Security Measures
Security	
Information	
Network	

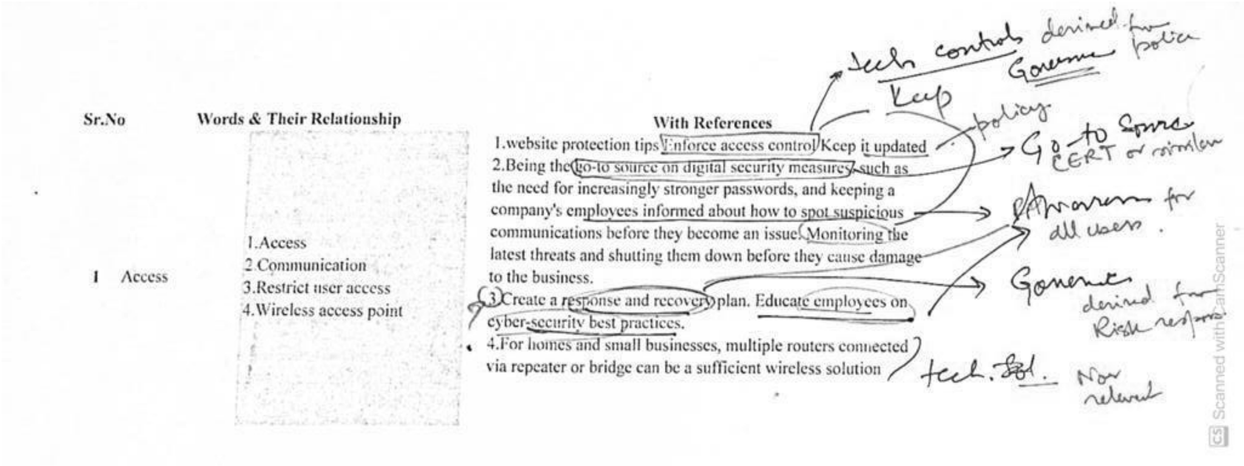
After consolidating the main categories and reducing them to six key words that were derived from the text, the original text was revisited and analyzed to understand the intended meaning and context of the response. Coupled with analytical questioning and memo writing, this enriched our understanding of their response and thus the generalized concepts of cybersecurity practices, as implemented in the respondents' organizations, were articulated with the help of a domain expert to validate them. While going through this exercise various modifications to the classification of the entities/codes was done after through deliberations and discussions, resulting in revisions and modifications of the categories and their derived meanings. The table 6 shows an initial category, the intermediate codes and the original text from where it was derived.

Table 1: Initial category, Intermediate codes and original text

Sr. No		Words & Their Relationship	With References
1	Access	1.Access 2.Communication 3.Restrict user access 4.Wireless access point	1. Website protection tips Enforce access control Keep it updated 2. Being the go-to source on digital security measures, such as the need for increasingly stronger passwords, and keeping a company's employees informed about how to spot suspicious communications before they become an issue. Monitoring the latest threats and shutting them down before they cause damage to the business. 3. Create a response and recovery plan. Educate employees on cyber-security best practices. 4.For homes and small businesses, multiple routers connected via repeater or bridge can be a sufficient wireless solution

Constant comparison of the categories intermediate codes and original text led to the revised categories. An exemplar is given in Table 6.

Further, the original text in light of the deliberations helped in extracting the generalized strategies in vogue in small businesses. The highlights an instance of it is mentioned in figure 2.



Sr.No		Words & Their Relationship	With References
1	Access	1.Access 2.Communication 3.Restrict user access 4.Wireless access point	1.website protection tips Enforce access control Keep it updated 2.Being the go-to source on digital security measures, such as the need for increasingly stronger passwords, and keeping a company's employees informed about how to spot suspicious communications before they become an issue. Monitoring the latest threats and shutting them down before they cause damage to the business. 3.Create a response and recovery plan. Educate employees on cyber-security best practices. 4.For homes and small businesses, multiple routers connected via repeater or bridge can be a sufficient wireless solution

Figure 2: The original text from where generalized strategies are extracted

4.2. Data Interpretation

Data analysis and interpretation done on the extracted categories with constant comparison to the original text. To demonstrate this let us look at the first category: Access. The words derived from the text include:

1.Access 2.Communication 3.Restrict user access 4.Wireless access point

Then based on constant comparison of the above words and the derived category, the original text is analyzed to get a generalized understanding of the response as shown in the Table 7.

Table 7: Derived understanding and generalized understanding

Original text	Derived understanding	generalized understanding
1 website protection tips Enforce access control Keep it updated	Technical controls/policy	Cybersecurity Governance can ensure protection.
2. Being the go-to source on digital security measures, such as the need for increasingly stronger passwords, and keeping a company's employees informed about how to spot suspicious communications before they become an issue. Monitoring the latest threats and shutting them down before they cause damage to the business.	go-to source Educating employees Policy decision	Go-to source of cyber security technical support. Cybersecurity Awareness of employees and users. Cybersecurity Governance can ensure protection
3. Create a response and recovery plan. Educate employees on cyber-security best practices.	Policy decision Educating employees	Cybersecurity Governance can ensure protection
4. For homes and small businesses, multiple routers connected via repeater or bridge can be a sufficient wireless solution	Technical solution	*This is not relevant as it is not about cybersecurity*

The detailed analysis of category Access has revealed that there are three points of understanding of cybersecurity and the strategies used in small businesses listed below in Table 8:

Table 8: Generalized Understanding and Cybersecurity

Generalized Understanding	Cybersecurity Strategy
Cybersecurity Governance can ensure protection.	Establish cybersecurity governance system to provide an all-encompassing high level protection.
Go-to source of cyber security technical support	A readily accessible cybersecurity technical experts team with adequate resources be available to the employees/users
Cybersecurity Awareness of employees and users	Ensuring Cybersecurity awareness for all employees is a must.

The similar process is applied to the rest of the categories to arrive at the points of understanding of cybersecurity and the strategies used in small businesses. It may be noted that there are instances where the same piece of text has been used to derive different codes and categories. However, during analysis and interpretation, constant comparison guides the process of understanding and eliminates any redundancies.

Resulting strategies from the data collected through questionnaire responses are listed below in Table 9.

Table 9: Resulting Strategies

Table 9: Resulting Strategies

Cybersecurity Strategy	**Remarks**
1. Establish cybersecurity governance system to provide an all-encompassing high level protection.	An enhanced understanding of this strategy has evolved as #6.
2. A readily accessible cybersecurity technical experts team with adequate resources be available to the employees/users	
3. Ensuring Cybersecurity awareness for all employees is a must.	
4. First thing to do is to list all the digital assets as they are valuable and must be protected.	An enhanced understanding of this strategy has evolved as #7.
5. Technical security measure are required for protection.	
6. Establish cybersecurity governance system with the objective to secure organization's digital assets to provide an all-encompassing high level protection	
7. First thing to do is to list all the digital assets including data as they are valuable and must be protected.	
8. First thing to do is to list all the digital assets including data, especially the sensitive business information, as they are valuable and they must be protected.	

Final list of strategies is given in table 10:

Table 10: Final list of cybersecurity strategies

Cybersecurity Strategy
1. A readily accessible cybersecurity technical experts team with adequate resources be available to the employees/users
2. Ensuring Cybersecurity awareness for all employees is a must.
3. Technical security measure are required for protection.
4. Establish cybersecurity governance system with the objective to secure organization's digital assets to provide an all-encompassing high level protection
5. First thing to do is to list all the digital assets including data, especially the sensitive business information, as they are valuable and they must be protected.

4.3. Saturation of the Results and Recommendations

To get further insights for improving our understanding of the topic and enriching the resultant list of strategies guided interviews were held. The data collected from recording the interviews. The analysis, interpretation and selective coding with constant comparison of interview data with the existing strategies extracted and listed in Table 8 in previous section, revealed that there was no further insights to be gained. Thus, the saturation point was reached.

The resulting strategies are listed below in Table 11 in the order of importance:

Table 11: Cybersecurity Strategies in order of importance

Cybersecurity Strategy
1. First thing to do is to list all the digital assets including data, especially the sensitive business information, as they are valuable and they must be protected.
2. Establish cybersecurity governance system with the objective to secure organization’s digital assets to provide an all-encompassing high-level protection
3. Technical security measure are required for protection.
4. Ensuring Cybersecurity awareness for all employees is a must.
5. A readily accessible cybersecurity technical experts team with adequate resources be available to the employees/users

1. First thing to do is to list all the digital assets including data, especially the sensitive business information, as they are valuable, and they must be protected.

This is the most important point to understand. An organization needs to know what all digital artifacts it has that are valuable to be classified as assets. These should include the sensitive business information that an organization is keeping with it. It can include employee, customer, partner, financial and personal data among others. Once this list of digital assets is available the value of this data and the potential loss in case of breach of data can be quantified and the cost of cybersecurity system can be compared and offset against the value of it.

2. Establish cybersecurity governance system with the objective to secure organization’s digital assets to provide an all-encompassing high-level protection.

Most people, especially the technical and cybersecurity specialists tend to think that there is a technical solution to all the cybersecurity challenges. However, there are other more important issues to be settled before jumping to the technical solutions. These include but are not limited to answers to the questions like:

Who owns the data? What is the value of our digital assets? What level of protection should be provided to these digital assets? How can the protection be ensured? Who is responsible in case of cybersecurity breach? Etc. These are all related to Cybersecurity Governance. Policies, procedures and systems with the objective of securing digital assets are derived from and overarching and comprehensive cybersecurity governance system.

3. Technical security measures is required for protection.

The technical security measures is essential for providing any meaningful security to the digital assets of an organization. These are costly and require specialized skills to be deployed and constant upgrade are required as new threats are discovered.

4. Ensuring Cybersecurity awareness for all humans (employees, customers, partner etc.) is a must.

Even the best and latest technological solutions deployed in an organization can be rendered useless and vulnerable by the humans. The cybersecurity breaches have a human factor attributing to the breach (Milkovich 2020).The non-technical end users, the technical users and even the cybersecurity experts are at the end humans and have physical, psychological, emotional, ethical and social limitation innate to the humans. Thus, cybersecurity sensitization, cyber hygiene, and cybersecurity awareness has to be provided. Considering the detrimental effects of unaware users, the EU has funded a three-year (2021-2024) capacity building project titled ‘Rethinking Cybersecurity in Pakistan: Human factors’ Essential Role (ReCyP:HER) to create cybersecurity awareness among users. The results of this research will provide insights to the researchers of this project to help them design and develop Cybersecurity Awareness camping and contents for dissemination among the users to better inform and educate them regarding the cyber threats. The awareness campaigns must be a regular feature that is repeated whenever new threat and vulnerabilities are discovered and when on-boarding any employee. The top management must not be left out and be included in these awareness campaigns and trainings.

5. A readily accessible cybersecurity technical experts team with adequate resources be available to the employees/users

Cyber-attack or cybersecurity breach is not an issue of if but a matter of when. Therefore, whenever it strikes, the users must have a go-to resource of readily accessible team of cybersecurity technical experts. This team should be adequate supported with all the necessary resources, open and welcoming to the users. The users should be aware of their existence in the organization and the place/procedure to quickly access them.

As a recommendation we suggest that Cybersecurity is a highly specialized domain requiring constant upgrade in technology, skills and awareness. It is expensive and requires large budget. Small business might find it difficult to have in-house capabilities and skills to manage an effective cybersecurity posture. While the governance can be kept in-house, the business can consider outsourcing the technical side of the cybersecurity solution. Manager technical solution with adequate cyber protection offered by third parties may be a more cost-effective and robust than a minimally skilled and funded part-time in-house solution. The cybersecurity awareness and a go-to resource in case of cybersecurity breach should be outsourced to provide a professional support and delivery.

5. Conclusion

Small business owners struggle to keep their company data safe and secure from external threats. Online systems and services have expanded business opportunities, especially for the small businesses, at the same time it has increased the vulnerability of the system to targets by criminals/hackers. Due to lack of resources as the businesses are being small, they do not focus the cyber security threats. The sensitive business information combined with other data is made available as a high prized digital assets (Günther, Glas, and Poddig 2022; Glas 2022; Su 2020) by the businesses going online. This has become a lucrative target of the cyber criminals. Therefore, the digital assets and the infrastructure needs to be safeguarded.

The aim is to add knowledge to fill the gap in business practice related to cyber security policies in small businesses. Small business, who lack adequate cyber security strategies to protect information systems from cyber threats could benefit from this study. The survey followed-up by interview of executives from small businesses shall help understand the research problem.

The initial responses are collected from the participant through an online questionnaire with both closed and open-ended questions. Exploration of the data from each online questionnaire allowed us to construct the overarching themes to develop a categorical code database. A combination of the data from all participants revealed consistent patterns. Synthesizing the topics provided a full picture of the data collected regarding the research question.

Grounded Ontology (GO) method which consists of five steps is used to extract the key words and its reference. These key words are further to extract the generalized and derived understanding for policy recommendations.

The results suggest that cybersecurity is a highly specialized domain requiring constant upgrade in technology, skills, and awareness. Small business might find it difficult to have in-house capabilities and skills to manage an effective cybersecurity posture. The cybersecurity awareness and a go-to resource in case of cybersecurity breach should be outsourced.

This is an exploratory case-study based research and the results are just preliminary insights to guide an in-depth research and treatment of the research topic and questions. Thus, these results are by no means definitive. However, these results can serve as a base line understanding about the cybersecurity strategies employed by small businesses. For further research, one can incorporate triangulation and inter-coder reliability factor to enhance the validity of the study. The inter-coder reliability can be established through data analysis and interpretation jointly with a cybersecurity expert. Although, it introduced another limitation of groupthink psychological bias, yet, due to the time constraint it helped get some meaningful results.

Reference

Ademola, Ojo E. 2022. "Multi-Stakeholder Security Governance Scaling for Cyber Security."

Akintoye, Rufus, Olubunmi Ogunode, Modupe Ajayi, and Abimbola Abosede Joshua. 2022. "Cyber Security and Financial Innovation of Selected Deposit Money Banks in Nigeria."

Alazab, Mamoun, Swarna Priya RM, M. Parimala, Praveen Kumar Reddy Maddikunta, Thippa Reddy Gadekallu, and Quoc-Viet Pham. 2021. "Federated Learning for Cybersecurity: Concepts, Challenges, and Future Directions." IEEE Transactions on Industrial Informatics 18 (5). IEEE: 3501–9.

Alber, Nader. 2020. "The Effect of Coronavirus Spread on Stock Markets: The Case of the Worst 6 Countries." Available at SSRN 3578080.

Al-Ghamdi, Mohammed I. 2021. "Guide to Developing a National Cyber Security Strategy." Materials Today: Proceedings. Elsevier.

Allam, Zaheer. 2019. "The Emergence of Anti-Privacy and Control at the Nexus between the Concepts of Safe City and Smart City." Smart Cities 2 (1). MDPI: 96–105.

2020. Urban Governance and Smart City Planning: Lessons from Singapore. Emerald Group Publishing.

AL-Nuaimi, Maryam Nasser. 2022. "Human and Contextual Factors Influencing Cyber-Security in Organizations, and Implications for Higher Education Institutions: A Systematic Review." Global Knowledge, Memory and Communication, no. ahead-of-print. Emerald Publishing Limited.

Aurelien, Joubert. 2021. "Exploring Effective Defensive Cybersecurity Strategies for Small Businesses." PhD Thesis, Colorado Technical University.

Behera, Rajat Kumar, Pradip Kumar Bala, Nripendra P. Rana, and Hatice Kizgin. 2022. "Cognitive Computing Based Ethical Principles for Improving Organisational Reputation: A B2B Digital Marketing Perspective." Journal of Business Research 141. Elsevier: 685–701.

Benoliel, Daniel. 2014. "Towards a Cybersecurity Policy Model: Israel National Cyber Bureau Case Study." NCJL & Tech. 16. HeinOnline: 435.

Bernik, Igor. 2014. "Cybercrime: The Cost of Investments into Protection." Varstvoslovje: Journal of Criminal Justice & Security 16 (2).

Brangetto, Pascal, and M. K. S. Aubyn. 2015. "Economic Aspects of National Cyber Security Strategies." Brangetto P., Aubyn MK-S. Economic Aspects of National Cyber Security Strategies: Project Report. Annex 1 (9–16): 86.

Christensen, Kristoffer Kjærgaard, and Tobias Liebetrau. 2019. "A New Role for 'the Public'? Exploring Cyber Security Controversies in the Case of WannaCry." Intelligence and National Security 34 (3). Taylor & Francis: 395–408.

Cristiano, Fabio. 2021. "Israel: Cyber Defense and Security as National Trademarks of International Legitimacy." Routledge Companion to Global Cyber-Security Strategy. Routledge, 409–17.

Dalal, Reeshad S., David J. Howard, Rebecca J. Bennett, Clay Posey, Stephen J. Zaccaro, and Bradley J. Brummel. 2022. "Organizational Science and Cybersecurity: Abundant Opportunities for Research at the Interface." Journal of Business and Psychology 37 (1). Springer: 1–29.

Deora, Raj Singh, and Dhaval Chudasama. 2021. "Brief Study of Cybercrime on an Internet." Journal of Communication Engineering & Systems 11 (1): 1–6.Eling, Martin, Mauro Elvedi, and Greg Falco. 2022. "The Economic Impact of Extreme Cyber Risk Scenarios." North American Actuarial Journal. Taylor & Francis, 1–15.

Farias, Bruno Graebin de, Luciana Dutra-Thomé, Silvia Helena Koller, and Thiago Gomes de Castro. 2021. "Formulation of Themes in Qualitative Research: Logical Procedures and Analytical Paths." Trends in Psychology 29 (1). Springer: 155–66.

Firmansyah, Asep Fajar, Qurrotul Aini, Akhmad Saehudin, and Siti Amsariah. 2020. "Information Security Awareness of Students on Academic Information System Using Kruger Approach." In 2020 8th International Conference on Cyber and IT Service Management (CITSM), 1–7. IEEE.

Ghobakhloo, Morteza, and Sai Hong Tang. 2013. "The Role of Owner/Manager in Adoption of Electronic Commerce in Small Businesses: The Case of Developing Countries." Journal of Small Business and Enterprise Development. Emerald Group Publishing Limited.

Gill, Charlotte, David Weisburd, Cody W. Telep, Zoe Vitter, and Trevor Bennett. 2014. "Community-Oriented Policing to Reduce Crime, Disorder and Fear and Increase Satisfaction and Legitimacy among Citizens: A Systematic Review." Journal of Experimental Criminology 10 (4). Springer: 399–428.

Glas, Tobias. 2022. "Digital Assets." In Asset Pricing and Investment Styles in Digital Assets, 47–93. Springer.

Glaser, Barney G., and Anselm L. Strauss. 2017. The Discovery of Grounded Theory: Strategies for Qualitative Research. Routledge.

Goel, Sanjay. 2020. "National Cyber Security Strategy and the Emergence of Strong Digital Borders." Connections 19 (1). JSTOR: 73–86.

Goode, Sigi, Hartmut Hoehle, Viswanath Venkatesh, and Sue A. Brown. 2017. "User Compensation as a Data Breach Recovery Action: An Investigation of the Sony PlayStation Network Breach." MIS Quarterly 41 (3): 703–27.

Gorian, Ella V. 2020. "Information Security at ASEAN in a Digitalized Economy: National and Regional Approaches." Laplage Em Revista 6 (Extra-A): 214–21.

Günther, Steffen, Tobias Glas, and Thorsten Poddig. 2022. "Asset Pricing in Digital Assets." Universität Bremen.

Hamilton, Stuart, Alex Byrne, and Susanne Seidelin. 2002. "The Internet: The Information Tool of the 21st Century." Libraries, Conflicts 171 (727.360): 23–56.

Harsch, Alexander, Steffen Idler, and Simon Thurner. 2014. "Assuming a State of Compromise: A Best Practise Approach for SMEs on Incident Response Management." In 2014 Eighth International Conference on IT Security Incident Management & IT Forensics, 76–84. IEEE.

Hou, Rui, Guowen Ren, Chunlei Zhou, Hongxuan Yue, Huan Liu, and Jiayue Liu. 2020. "Analysis and Research on Network Security and Privacy Security in Ubiquitous Electricity Internet of Things." Computer Communications 158. Elsevier: 64–72.

Huang, Hsini. 2020. "A Collaborative Battle in Cybersecurity? Threats and Opportunities for Taiwan." Asia Policy 27 (2). National Bureau of Asian Research: 101–6.

Huang, Hsini, and Tien-Shen Li. 2018. "A Centralised Cybersecurity Strategy for Taiwan." Journal of Cyber Policy 3 (3). Taylor & Francis: 344–62.

Idahosa, Martins Donbruce. 2020. "Strategies for Implementing Successful IT Security Systems in Small Businesses." PhD Thesis, Walden University.

Izycki, Eduardo, and Rodrigo Colli. 2019. "Protection of Critical Infrastructures in National Cyber Security Strategies." In ECCWS 2019-Proceedings of the 18th European Conference on Cyber Warfare and Security.

Kamin, Daud A. 2017. "Exploring Security, Privacy, and Reliability Strategies to Enable the Adoption of IoT." PhD Thesis, Walden University.

Khan, Navid Ali, Sarfraz Nawaz Brohi, and Noor Zaman. 2020. "Ten Deadly Cyber Security Threats amid COVID-19 Pandemic." TechRxiv.

Khan, Shah Khalid, Nirajan Shiwakoti, and Peter Stasinopoulos. 2022. "A Conceptual System Dynamics Model for Cybersecurity Assessment of Connected and Autonomous Vehicles." Accident Analysis & Prevention 165. Elsevier: 106515.

Kim, Elizabeth, D. Gardner, S. Deshpande, R. Contu, D. Kish, and C. Canales. 2018. "Forecast Analysis:

Information Security, Worldwide, 2Q18 Update." Gartner Research.

Kosseff, Jeff. 2020. "Hacking Cybersecurity Law." U. Ill. L. Rev. HeinOnline, 811.

Lallie, Harjinder Singh, Lynsay A. Shepherd, Jason RC Nurse, Arnau Erola, Gregory Epiphaniou, Carsten Maple, and Xavier Bellekens. 2021. "Cyber Security in the Age of COVID-19: A Timeline and Analysis of Cyber-Crime and Cyber-Attacks during the Pandemic." Computers & Security 105. Elsevier: 102248.

Leedy, Paul D., and Jeanne Ellis Ormrod. 2015. Practical Research: Planning and Design. Pearson.

Li, Yuchong, and Qinghui Liu. 2021. "A Comprehensive Review Study of Cyber-Attacks and Cyber Security; Emerging Trends and Recent Developments." Energy Reports 7. Elsevier: 8176–86.

Liveri, Dimitra, Anna Sarri, and Eleni Darra. 2018. "ENISA's Contribution to National Cyber Security Strategies." In Cybersecurity Best Practices, 43–64. Springer.

Luiijf, Eric, Kim Besseling, and Patrick De Graaf. 2013. "Nineteen National Cyber Security Strategies." International Journal of Critical Infrastructures 6 9 (1–2). Inderscience Publishers Ltd: 3–31.

Luiijf, H. A. M., Kim Besseling, Maartje Spoelstra, and Patrick de Graaf. 2011. "Ten National Cyber Security Strategies: A Comparison." In International Workshop on Critical Information Infrastructures Security, 1–17. Springer.

Michalec, Ola Aleksandra, Dirk Van Der Linden, Sveta Milyaeva, and Awais Rashid. 2020. "Industry Responses to the European Directive on Security of Network and Information System: Understanding Policy Implementation Practices across Critical Infrastructures." In Sixteenth Symposium on Usable Privacy and Security (SOUPS 2020), 301–17.

Milkovich, Devon. 2020. "Alarming Cyber Security Facts and Stats." Cybint Solutions.

Myftari, Kledian. 2021. "Beyond the Impasse: Prospects for Joint Cooperation between Russia and the US in Cybersecurity." Univerzita Karlova, Fakulta sociálních věd.

Nabi, Syed Irfan. 2013. "Grounded Ontology–A Text Coding Approach to Ontology Development for Human Behavior Aspects of Information Security." PhD Thesis, Institute of Business Administration, Karachi, Pakistan.

Nanto, Dick K. 2009. The Global Financial Crisis: Analysis and Policy Implications. Diane Publishing.

Nifakos, Sokratis, Krishna Chandramouli, Charoula Konstantina Nikolaou, Panagiotis Papachristou, Sabine Koch, Emmanouil Panaousis, and Stefano Bonacina. 2021. "Influence of Human Factors on Cyber Security within Healthcare Organisations: A Systematic Review." Sensors 21 (15). MDPI: 5119.

Osho, Oluwafemi, and Agada D. Onoja. 2015. "National Cyber Security Policy and Strategy of Nigeria: A Qualitative Analysis." International Journal of Cyber Criminology 9 (1). International Journal of Cyber Criminology: 120.

Parkinson, Simon, and Saad Khana. 2022. "Identifying High-Risk over-Entitlement in Access Control Policies Using Fuzzy Logic." Cybersecurity 5 (1). SpringerOpen: 1–17.

Pauletto, Christian. 2020. "Information and Telecommunications Diplomacy in the Context of International Security at the United Nations." Transforming Government: People, Process and Policy 14 (3). Emerald Publishing Limited: 351–80.

Percy, William H., Kim Kostere, and Sandra Kostere. 2015. "Generic Qualitative Research in Psychology." The Qualitative Report 20 (2). Citeseer: 76–85.

Pranggono, Bernardi, and Abdullahi Arabo. 2021. "COVID-19 Pandemic Cybersecurity Issues." Internet Technology Letters 4 (2). Wiley Online Library: e247.

Rajan, Rishabh, Nripendra P. Rana, Nakul Parameswar, Sanjay Dhir, and Yogesh K. Dwivedi. 2021. "Developing a Modified Total Interpretive Structural Model (M-TISM) for Organizational Strategic Cybersecurity Management." Technological Forecasting and Social Change 170. Elsevier: 120872.

Ron, Mario, Geovanni Ninahualpa, David Molina, and Javier Díaz. 2020. "How to Develop a National Cybersecurity Strategy for Developing Countries. Ecuador Case." In International Conference on

Information Technology & Systems, 553–63. Springer.

Sayin, Muhammed O., and Tamer Başar. 2017. “Secure Sensor Design for Cyber-Physical Systems against Advanced Persistent Threats.” In International Conference on Decision and Game Theory for Security, 91–111. Springer.

Senol, Mustafa, and Ertugrul Karacuha. 2020. “Creating and Implementing an Effective and Deterrent National Cyber Security Strategy.” Journal of Engineering 2020. Hindawi.

Shackelford, Scott J. 2019. “Should Cybersecurity Be a Human Right: Exploring the Shared Responsibility of Cyber Peace.” Stan. J. Int’l L. 55. HeinOnline: 155.

Shafqat, Narmeen, and Ashraf Masood. 2016. “Comparative Analysis of Various National Cyber Security Strategies.” International Journal of Computer Science and Information Security 14 (1). LJS Publishing: 129.

Song, Ligang, and Yixiao Zhou. 2020. “The COVID-19 Pandemic and Its Impact on the Global Economy: What Does It Take to Turn Crisis into Opportunity?” China & World Economy 28 (4). Wiley Online Library: 1–25.

Su, Eva. 2020. Digital Assets and SEC Regulation. Congressional Research Service.

Tehrani, Pardis Moslemzadeh, Nazura Abdul Manap, and Hossein Taji. 2013. “Cyber Terrorism Challenges: The Need for a Global Response to a Multi-Jurisdictional Crime.” Computer Law & Security Review 29 (3). Elsevier: 207–15.

Ter, Kah Leng. 2018. “Singapore’s Cybersecurity Strategy.” Computer Law & Security Review 34 (4): 924–27. doi:10.1016/j.clsr.2018.05.001.

Wan, Ming, Jiawei Li, Ying Liu, Jianming Zhao, and Jiushuang Wang. 2021. “Characteristic Insights on Industrial Cyber Security and Popular Defense Mechanisms.” China Communications 18 (1). IEEE: 130–50.

Wang, Ping, and Christopher Johnson. 2018. “Cybersecurity Incident Handling: A Case Study of the Equifax Data Breach.” Issues in Information Systems 19 (3).

Wang, Ping, and Sun-A. Park. 2017. “COMMUNICATION IN CYBERSECURITY: A PUBLIC COMMUNICATION MODEL FOR BUSINESS DATA BREACH INCIDENT HANDLING.” Issues in Information Systems 18 (2).

Yee, Chai Kar, and Mohamad Fadli Zolkipli. 2021. “Review on Confidentiality, Integrity and Availability in Information Security.” Journal of ICT in Education 8 (2): 34–42.

Zimmermann, Verena, and Karen Renaud. 2019. “Moving from a ‘human-as-Problem” to a ‘human-as-Solution” Cybersecurity Mindset.” International Journal of Human-Computer Studies 131. Elsevier: 169–87.

Żywio\lek, Justyna, Joanna Rosak-Szyrocka, and Borut Jereb. 2021. “Barriers to Knowledge Sharing in the Field of Information Security.” Management Systems in Production Engineering.