The effect of cybersecurity training on achieving sustainable development goals

Author: Levente Budai
University of Twente
P.O. Box 217, 7500AE Enschede
The Netherlands

ABSTRACT,
In today's technological landscape, the increasing adoption of digital practices has urged companies to embrace new technologies that let them compete in the modern business world. This trend also enabled the adoption of sustainable innovations, placing further emphasis on a green future. However, this widespread digitalization has also introduced significant technological risks threatening the digital environment. To address the growing technological challenges, an increasing number of organizations are investing in cybersecurity training, which also evolves alongside the dangers it is trying to mitigate. The connection between cybersecurity training and sustainability objectives is a relatively new area of study, which is why the paper aims to cover the link between the abovementioned variables. This study investigates the relationship through the lens of qualitative research, with the help of semi-structured interviews. The interviews covered multiple organizations and industries and the data gathered was analyzed using an inductive approach to find real-world examples and recognizable patterns. The research revealed that cybersecurity and awareness training offer additional benefits to organizations beyond their original goals of countering cybersecurity threats. Even if the link between cybersecurity training and sustainability goals is not a direct one, preventative measures in the field of cybersecurity contribute to cost savings by mitigating the damage associated with successful cyberattacks, while also enabling a shift to digital processes and an online work environment, both of which require less capital investment. The paper dives deeper into the connection between cybersecurity training and sustainable goals and proposes a conceptual model connecting real-world aspects.

Graduation Committee members:

Dr. Pauline Weritz
Dr. Rashimah Rajah

Keywords
Cybersecurity, Cybersecurity Training, Sustainability, SDGs, Digitalization, Semi-structured Interviews, Thematic Analysis, and Qualitative Research

This is an open access article under the terms of the Creative Commons Attribution License, which permits use, distribution, and reproduction in any medium, provided the original work is properly cited.

CC-BY-NC

1. INTRODUCTION

Twin transition is characterized by the simultaneous transformation of sustainability and technology in an organizational context (Stratmann, 2022). Both aspects enjoyed a recent, wide-spread development due to the impact of Covid-19 (Christmann et al., 2024). The increased awareness for more sustainable products, as well as the shift towards online customer presence brought new approaches forward, to be adopted by the organizations (Primorac et al., 2022). This new, digital age led to digital transformation and innovation in the field of technology. Restrictions proposed by the government around the globe accelerated the adoption of technological improvements, to combat the limitations caused by the Pandemic (McKinsey & Company, 2020). These circumstances created the prime opportunity for online business to flourish in, with e-commerce spendings reaching a 55% increase in the United States, during the pandemic, according to Adobe (Mitchell, 2022). These changes did not stop with the customers, as more and more employees started working from home to limit the contact they have with the outside world. These technological developments gave rise to digitalization, which in turn enabled organizations to adapt to the rapid changes in the environment (Parker et al., 2022). However, digitalization also brought forward the negative aspects of wide-spread technology.

With the escalation of digitalization in a data-driven world, cyber-related risks materialized as a worldwide concern, with the average cost of a data breach now estimated at $4.45m (Gaudin, 2023). There are many instances in recent history, where cyber-attacks resulted in major damage to organizations in various forms, such as damage to reputation via negative public image, or loss of customer trust; (Under Armor 2018), financial loss through theft or disruption of operations; (Best Buy 2017), information leakage (Rockstar 2024) and legal consequences (Verizon 2022; Uber 2016). As the business operations of organizations contain the use of assets and data, they become exposed to increasingly evolving security concerns, that can disrupt their daily activities (Weishäupl et al., 2015). Therefore, it is crucial for organizations to adequately utilize their capabilities to prevent and respond to cybersecurity incidents.

With said cybersecurity incidents being on the rise, both in numbers and in damage done, organizations should start associating climate resiliency with cyber resiliency (Hossain, 2023)

Several papers link sustainable development (SD) and cybersecurity. Sulich (2023) presents an argument that both concepts need to be integrated to achieve sustainable, equitable, and secure economic growth. In an earlier study, Sulich and Rutkowska (2021) refer to the intersection of sustainable development and cybersecurity as 'Green Cybersecurity. The implementation of Green Cybersecurity was analyzed concerning the Environmental Goods and Services Sector (EGSS), with the results showcasing the positive relationship between the introduction of cybersecurity and sustainable development goals (SDGs) being achieved. Sustainable objectives related to the digital environment often include aspects related to data security, such as the 2030 agenda, which centers around data-driven governance (ElMassah et al., 2020). This example also connects cybersecurity to sustainable development goals, under the notion of data security. Moreover, other contemporary literature reviews about Industry 4.0 also highlighted the existent connection between sustainable development and cybersecurity. However, cyber-related risk can harm both aspects, with recent instances such as the Colonial Pipeline ransomware attack (May 6, 2021), or the North Korean state-sponsored espionage (14 April 2022) demonstrating the destructive consequences of cyber-attacks on the tangible environment (University of Hawaii, 2022; HHS Cybersecurity program 2021).

Cyberattacks take many forms and have different objectives, the most common ones being theft or destruction. Prakash (2019) highlighted the different types of cyberattacks and how they lead to casualties. The most well-known threats that cause harm to organizations include DDoS attacks, which deny access to the host, making it unavailable to use. Another common threat is phishing attacks, that aim to offload malware into the host software via malicious links or emails. Lastly, malware, often known as the common virus, which can interrupt certain computing operations or steal sensitive information or any other user data by discussing itself as legitimate code. These examples are meant to highlight the variety of ways organizations can suffer from cyberattacks and the potential risks they are exposed to in a digital environment.

Consequently, studies showcase the evolution of cyber-attacks over the years. According to a study by IBM Citi GPS (2023), "cyber-related incidents are on the rise, with the average estimated cost of a cyberattack surged to $4.24 million in 2021, 12% higher than its 2015 level and 10% higher compared with 2020 (p.10)". Moreover, the frequency and complexity of such attacks also improved over the last decade. The same study cites human error as the leading cause of cyber-related risks, while The Verizon 2022 Data Breach Investigation Report finds that 82% of data breach incidents involve a human component (Verizon, 2022). Human error can be seen as the lack of or any unintentional action that leads to a security breach. (Ahola, 2022). With the human aspect playing such a pivotal role in the eyes of cybersecurity, it becomes increasingly important for individuals to receive proper education toward safe online behavior (He et al., 2019).

Said education in an organizational setting comes in the form of employee training. These programs are designed to raise awareness and prepare employees to handle cybersecurity challenges (NIST, 2008). One of the most prominent forms of education comes from SETA programs, which primarily focuses on behavioral changes and mitigating cybersecurity risks. Cybersecurity education training and awareness (SETA) is defined by (Hu et al., 2021) as a form of organizational initiative,

which attempts to "focus employee attention on cyber security–related issues, provide employees with crucial knowledge and skills, enable their deep understanding of why security protection is needed, and increase their awareness of security issues" (p.752). SETA and other similar endeavors have become widely adopted by companies, with analysts also reporting an increase in spending on SETA or other related programs from 2020 onward (Cybersecurity Ventures, 2021). Similarly, other outlets report that the majority of Chief Information Security Officers consider employee training to be among the most prominent requirements for organizational cyber safety (BT Security, 2021; Financial Services Information Sharing and Analysis Center, 2018).

Following the previously established relationship between SDGs and cybersecurity, along with the growing presence of cyberattacks, we look towards the root cause of human error. More precisely, how reducing, or eliminating human error in the form of cybersecurity training affects the organizations' ability to achieve its sustainable development goals.

How does the implementation of cybersecurity training contribute towards organizations achieving sustainable development goals (SDGS)?

By conducting qualitative research, the study aims to investigate the relationship between cybersecurity training and sustainability goals with the help of semi-structured interviews.

The study aspires to contribute to prior research by highlighting the causal relationship between cybersecurity threats and the implementation of cybersecurity training. In addition, examining the factors surrounding cybersecurity training and preventative measures that contribute to sustainable measures. Based on the findings, preventative practices complement sustainable performance, hence it is recommended for organizations operating in a digital environment to adopt said preventative practices.

The following parts of this study will discuss relevant literature (section 2), followed by the methodology (section 3), where the means of analysis will be explained. Section 4 focuses on the results gathered from the semi-structured interviews, and section 5 will deliver on practical and theoretical implications while considering the limitations of the study. The paper will be concluded with section 6, with the addition of the appendix and references found in sections 7 and 8.

2. THEORETICAL BACKGROUND

2.1 Conceptualizing Cybersecurity and Cybercrime

The theoretical background section of the study will concentrate on conceptualizing the variables within the research rather than depending on pre-existing frameworks because the article employs inductive reasoning. Cybersecurity is the first variable under consideration. Scholars cannot agree upon a single, comprehensive definition for the term cybersecurity because it encompasses several different concepts. Cybersecurity does, however, share one characteristic, which is its ability to defend against hazards associated with technology. In recent years, cybersecurity has been characterized as a multi-level term that helps prevent cyberattacks and data breaches, while aiding risk management (Wall, 2001). Said risks come in the form of cyber-risks, which can be caused by systematic and human factors alike, meaning that cybersecurity does not focus solely on machine-based threats (Cains et al., 2021). According to Böhme (2018), cyber risk is defined by programmable components and incorporates two important elements: technology and economy. According to this interpretation, cybersecurity encompasses every measure taken to eliminate cyber threats, be it through proactive defense or reactive measures taken after an assault.

For a more comprehensive definition, we turn towards the US-CERT (United States Computer Emergency Response Team), who view cybersecurity as a systematic concept, meaning it does not cover individual's need for cybersecurity, but rather it addresses the cybersecurity needs of the collective. Furthermore, the cybersecurity division of the Department of Homeland Security (DHS), also provides a detailed statement, which characterizes cybersecurity by the following actions:

"The activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification, or exploitation."

This definition of cybersecurity is applicable to the study, as it defines the term as a systematic concept, that is mainly concerned with protection. Moreover, the broadness of the definition makes it easier to account for the various ways in which companies employ cybersecurity training, given the different views adopted by different organizations on the subject.

2.2 Conceptualizing training in the cybersecurity field (SETA)

In the previous section, we defined the meaning of cybersecurity and the threats it protects us from. In this section, we follow up on cybersecurity to get closer to the variable we want to examine. From cybersecurity we turn our attention to training within the field, and conceptualize the variable, using its common way of adaptation, in the form of SETA programs. Information Security Education Training and Awareness, or SETA for short, represents a security training program that targets employees of an organization (D'Arcy et al., 2009). The program aims to improve employee awareness and behavior to adopt security practices (Tsohou et al. 2015; Whitman et al., 2008). Many contemporary studies highlight the effectiveness of SETA programs, such as one conducted by Kweon (2021), who examined a positive relationship between total SETA training time and employee compliance with safe cybersecurity behaviors.

Past iterations of implemented cybersecurity highlight the usage of a framework named CyTrONE (Cybersecurity Training and Operation Network Environment), which aims to automate training under an open-source framework (Shinoda et al., 2017). The CyTrONE framework provides a network that can be accessed by trainees, staff, white-collar hackers, and instructors alike to imitate a real-world scenario. This training method is built upon the theoretical aspects of cybersecurity education and follows the principles of Beuran (2016), who established requirements for an improved cybersecurity program.

The requirements highlighted the importance of matching content for the target audience while considering their skills. Furthermore, the training should be improved by adopting hands-on activities. Lastly, the training should be widely adopted and should have sufficient cost/performance characteristics to be effective and sustainable in the long run.

This paper uses SETA programs as a baseline to define cybersecurity training. However, some elements need to be highlighted, such as cybersecurity training encompasses both theoretical concepts as well as hands-on training as a means of practice for said concepts (Ošlejšek, 2021). Given the past iterations of cybersecurity training and the different approaches

for its improvement, this study considers cybersecurity training as any systematic practice adopted by organizations to prepare individuals to handle real-life risks associated with technology.

2.3 Defining Sustainable Development Goals

Sustainable development goals, or SDGs, are a set of objectives introduced by the United Nations in 2015, which include economic, social, and environmental targets to be met by the year 2030 (Schmidt-Traub et al., 2017). The agreement included 17 distinct goals featuring 193 countries. Organizations and companies also started to adopt said SDGs among other green initiatives for various reasons, including (Vinichenko, 2015): sustainable economic growth, cost reduction, and changing customer preferences. Said sustainable practices also gradually became part of the corporate culture, to raise awareness towards sustainable causes and to satisfy stakeholders outside the company (Kücükgül et al., 2022). Aligning these findings to an organizational level, this paper views SDGs as:

Any organizational-level objective which aims to fulfill corporate sustainability targets.

This definition provides a broad view, that helps the research account for any form of SDG present under the various organizations that might participate in the research.

2.4 Human Capital Theory

The link between cybersecurity and sustainability objectives examined in the introduction section cites data protection goals and other variables as a reason. However, the relationship can also be viewed through the employee's lens who participates in cybersecurity training. One applicable theory for this study is the human capital theory, which states that human capital is a measurement of human decision-making, rooted in cognitive psychology (Jovanovic, 1995). Based on this theory, there are a finite number of decisions in a situation and said decisions can be categorized into positive or negative choices an individual can make. The theory surrounding human capital comes from Mincer (1958) and Becker (1962), who believed that investing time and resources into a general skill will result in more positive choices for individuals. This phenomenon was examined in research (Lemieux, 2006), which identified a positive relationship between time invested into schooling as a human capital and higher earnings and wages. Simply put, the more resources spent on a skill (time in this case) lead to a beneficial outcome (higher wages). On the contrary, the absence of human capital results in poor decision-making, which was showcased in multiple studies, such as the case of financial decisions, highlighted by economic literature (Agarwal et al., 2009, Madrian et al., 2001). These studies revealed that the quality of financial decisions of individuals with limited knowledge on the subject is quite poor but can be improved via time investment.

Human capital theory can be applied to this study, based on the two variables of cybersecurity training and the organization's objective to achieve goals related to sustainability. Given that individual human capital can be increased via training, they might produce fewer human errors and be more knowledgeable about technological practices that in turn benefit the organization. The perceived relationship between these variables will be further discussed in the hypothesis section.

3. METHODOLOGY

3.1 Research Design

With cybersecurity training encompassing both human and technological aspects, qualitative research was conducted to further investigate the topic, in the form of semi-structured interviews. The approach was chosen due to qualitative interviewing becoming a key method to analyze subjects related to social sciences (Brinkmann, 2023). Moreover, qualitative research is meant to investigate real-life settings (Yin, 2015), thus possibly giving us a better understanding of the underlying aspects of cybersecurity training and SDGs. The qualitative interviews are aimed at questioning employees in managerial positions who implemented cybersecurity training within their respective organizations. Applying inductive reasoning allows us to record observations from employees, recognize certain patterns concerning the relationship between cybersecurity training implementation and SDGs, and draw a conclusion based on the collected data (Ketokivi et al.,2010).

As this research includes primary data collection, ethical approval was requested at the ethics committee BMS of the University of Twente.

3.2 Data collection and Sampling

The chosen sampling method for this study is the convenience sampling approach, which falls under the non-probability sampling methods. Based on this approach, units are selected by the easiness of their access (Czernek-Marszałek et al., 2024), regarding geographical proximity, availability at a given time, or willingness to participate. Given the limited nature of the sample, as the entire population could not be interviewed, heterogeneous purposive sampling was applied to provide a diverse range of participants. The sample size for non-probability sampling techniques depends on the nature of the study (Boddy, 2016). For semi-structured interviews, the sample size differs heavily due to subject matter, but given the qualitative nature of the research, additional data collection is recommended until the data saturates, meaning any additional data collected will not add any new information to the research (Saunders et al.,2012), which can occur even around 12 participants (Boddy, 2016).

7 semi-structured interviews were conducted under the study, with participants being selected under the following criteria. (1) *All interview participants should be familiar with cybersecurity or awareness training. (2) The interviewees should be of working age between the ages of 18 and 65. (3) The participants should work in a field in which digital processes are exercised.*

Following this criteria, 7 participants agreed to partake in the study and provide insight into their experiences. The participants represented a variety of companies from Hungary and Germany, as well as different positions involved in modern business. Table 3.2.1 highlights the distribution of the participants. The figure lists all the interviewees who participated in the research, while demonstrating surface-level information, to differentiate between them. Given the sensitive nature of personal data, only limited information will be shown, to protect the interests of the interview participant. Additionally, each participant proceeded with a questionnaire, containing around fifteen questions, following the introduction. The questionnaire was designed to shed light on real-world experiences and examples of cybersecurity training and sustainability objectives in a modern business environment. Said questionnaire can be found in the appendix, under Figure 8.2.

	Gender	Industry	Field of employment	Interview Length
Participant 1	Male	Airline industry	Enterprise architect	42 minutes
Participant 2	Male	Tech industry	Software engineer	30 minutes
Participant 3	Female	Railway industry	Product designer	48 minutes
Participant 4	Male	Tourism industry	Contractor	54 minutes
Participant 5	Male	Tech industry	Data engineer	51 minutes
Participant 6	Female	Healthcare industry	Data scientist	43 minutes
Participant 7	Male	Tech Industry	Cybersecurity educator	31 minutes

Figure 3.2.1 – Table of Participants

3.3 Data Analysis

A qualitative thematic analysis was used to interpret the data collected from the semi-structured interviews. Thematic analysis is a form of qualitative research method, which focuses on the identification and analysis of emerging themes. (Braun, 2006). This method is commonly used to analyze interviews or research conducted on focus groups (Liamputtong, 2009) making it applicable to the study. By applying thematic analysis, we are searching across the data set to identify repeated patterns of meaning (Braun, 2006). Axial coding is used to deconstruct the data and establish a connection between them (Boeije HR, 2009). This step is a contributing factor towards pattern recognition within the dataset, furthermore, Braun and Clarke (2006) list it as an important process to adopt during qualitative data analysis. Before analyzing the data, the structured interviews were recorded and transformed into writing. When the interviews were in a text-based form they were transferred to Atlas.ti, a digital tool specifically to handle qualitative data analysis. Here the interviews were coded according to the Gioia methodology, first implemented by Gioia & Pitre (1990) and refined by Corley & Gioia (2012). This method aims to group concepts and assign a theme to them on a higher systematic basis, which corresponds to the second-order or axial coding. After the secondary stage, the second-order codes were further clustered into an aggregate dimension, which targets more abstract concepts for a conceptual model.

4. RESULTS

The primary aim of this paper was to investigate the relationship between cybersecurity training and sustainability objectives. Based on Figure 5.1, shown in the discussion section of the report, the results can be clustered into 4 main aggregate dimensions, namely: Cybersecurity Threats, Technical Cybersecurity Measures, Training and Prevention, and Sustainable Performance. The following section examines these dimensions further, based on the semi-structured interviews.

4.1 Cybersecurity Threats

There were two distinct categories of threats considered by the interviewees, which were characterized as: external concerns and internal concerns, both of which will be discussed below.

4.1.1 External Concerns

External concerns were identified by participants as risk or danger factors that originate outside the organization. Based on Participant 1's statement: "*The security team usually brings examples from the outside…*".Participant 1's statement also continues by saying "*It can be phishing attacks or ransomware attacks, so you have to consider the external situations*" Additionally, many participants provided examples of specific types of threats with external sources such as Phishing attacks (Participants: 1,2,4,5), Ransomware attacks (Participants: 1 and 2), Online scams (Participants: 3,4,7). Participant 3 indicated that the number of similar attacks are on the rise: "*There is a growing number of wrongdoers and danger in this field, which is why I think cybersecurity is important to stop them. Besides at work I also personally encountered some of them*" Participant 5 stated: "*We work with a large EU database, where a lot of personal information can be found. If someone accesses the system, they can cause a lot of trouble, we are talking identity theft, or selling personal information*" These statements amplify the danger and risk associated with external cybersecurity attacks. Moreover, statements from the interviewees indicate that said attacks are more common to encounter on an organizational or even on a personal level.

4.1.2 Internal Concerns

Internal concerns are similar risk factors for an organization, with the difference being that said concerns come from within the system. These variables are often a result of incorrect human practice, which leads to systemic vulnerabilities. Participant 7 stated: "*Cybersecurity threats are very dangerous, but human mistakes can be just as costly. There's a difference on how we view these things, there should be a clear vision if the danger is from within or not*". This indicates a clear similarity between external and internal danger factors, while separating the two based on their origin. Participant 1 indicated: "*My opinion is that guidance and knowledge are the most important things, so if everyone knows what they are doing. When they don't know what to do or where to go, they feel frustrated, which obviously leads to full chaos, so of course we want to avoid such things*". These examples indicate an issue that derives from within the organization and can be avoided via training or other methods. By eliminating human error, or reducing the likelihood of internal flaws, the cybersecurity capabilities of the organization can be enhanced the same way when applying preventative or safety measures to protect the organization from outside danger.

4.2 Training and Prevention

This aggregate dimension encapsulates the measures taken by organizations to combat cybersecurity risks, with educational and preventative methods. Said measures include education methods, training outcomes, preventative measures, and protective measures.

4.2.1 Education Methods

Participants reported on a variety of training programs to enhance employee knowledge and competency to handle cybersecurity risks. Participant 1 stated: "*Training is not necessarily optional, so we have a plan based on the role of a person and what kind of training they must follow on a yearly basis. So based on the role we have a separate plan for let's say everyone so that's how it works in our case*". Participant 3 indicated a similar environment, where training is mandated for employees: "*The employer often requires the completion of e-learning courses for the employees. Examples like information and data safety, asset protection, etcetera…*". These examples showcase a more traditional educational approach towards protection, where the aim is to boost knowledge and awareness among employees. Participant 2 shared a dissimilar educational procedure, which implements practice attacks, for a more practical test for the employees: "*We have simulated phishing attacks, where they send you an email with a phishing link and their goal is for you to open the link, so they can infect the computer with it. They have other methods too, but I would say this one is the most common example*" This demonstrates a shift from a theoretical educational method, with the adoption of a life-like situation to prepare the employees for real-world threats. Another way to group employees for training

was indicated by Participant 4, who talked about knowledge-based separation when it comes to training: "*We have separate programs for age and knowledge. In our experience the older generation is not as up to date with technology as the digital nomads…*". Lastly, Participants 4 and 7 both reported awareness programs that were organized by third-party services, which offered knowledge-based training for the attendees. Awareness programs are mainly concerned with updating the pre-existing knowledge and reporting newly found risks and vulnerability points. Comparatively, the above-mentioned training methods fall under the category of workplace education. Organizations implement said education to enhance the technological proficiency of their employees and to prevent the likelihood of experiencing cyber-related concerns.

4.2.2 Training Outcomes

Training outcomes is a second-order theme, which aims to group the perceived results that follow the implemented training. Participant 3 reported: "*Education/Training is one of the pillars to greater knowledge that prepares colleges to take the adequate security steps*". Consequently, awareness or information training often results in a wider grasp of insights into technological vulnerabilities. This is often cited as a driving factor for the implementation of cybersecurity or awareness training and is often seen as the most common outcome of workplace education. On the other hand, Participant Two cited first-hand experience as their primary outcome, given the practical nature of their simulated training: "*When we get to experience a cyber-attack like simulation, it gives us a better idea of what it would look like in real life and what to look out for*". On another hand, Participant 7 highlighted the skillset of the colleagues: "*Those who participate often come out with more information, like what to avoid, or more skills that help them to deal with situations like these*". Their statement continues with: "We often see that they require less help around their computer, which also saves us time". Ultimately, the listed outcomes tie back to the individual training each participant received, which results in a small variation between the perceived outcomes of said training.

4.2.3 Preventative Measures

Through the semi-structured interviews, we found that many organizations that are involved with technology adopt preventative measures. These measures are in place to avoid the consequences of cyberattacks and are often presented as necessary practices in the digital field. An example features a statement from Participant 1: "*In our case, we want to be prepared for anything. We don't want to scare people, but we have to be aware that anytime anything can happen. There's an internal risk management protocol we follow to be ready for anything*". This shows the risk mitigation aspect of the preparation, which offers guiding principles to lessen the potential uncertainties surrounding technology. Another example of preventative measure is when Participant 2 lists quality control as a practice: "*We are always paying attention to the software we use, and we do regular maintenance on our servers so that they are up to date*". The third identified factor under the preventative theme came from Participant 3, who demonstrated the knowledge aspect of preparation, stating: "*Our cybersecurity team regularly updates us on our potential vulnerability points, and gives us feedback regarding our cyber defense*". As mentioned above, these practices' primary goal is to avoid certain attacks, and there are different types of approaches for each organization that fit their capabilities.

4.2.4 Protecting Measures

Protecting measures operate under a similar goal, which is to defend the valuables or assets of the organization from unregistered access or potential danger. Based on the findings the core difference between protection and preventative measures are the following:

- Preventative measures focus on reducing the likelihood of a certain unfavorable event and aim to reduce the success rate of incoming cybersecurity attacks, by using proactive measures
- Protecting measures refer to practices that aim to reduce the impact of cyberattacks, being a prime defense mechanism against digital threats

Based on the semi-structured interviews the following factors were identified: tactical protective measures, backup solutions, and incident response planning. Participant 1 stated: "*We have tactical protection, which includes a multi-factor login system and real-time network traffic monitoring, to make sure the access points are as secure as possible*". On another note, Participant 5 indicated the usage of an offline backup service, in case things go south. "*There is a backup option separate from the cloud, that stores information. If anything happens to the current information in the cloud, we resort to the backup that cannot be accessed through digital means*". Lastly Participant 6 highlighted the use of an incident response planning system by stating: "*The system in place tells us what to do and how to behave in case a data breach happens. We of course will try to recover the data, if possible, but these situations often require steps in more detail*".

4.3 Sustainable Performance

Alongside cybersecurity threats and cybersecurity training, data collected through the semi-structured interviews indicated the presence of variables under sustainable performance. The upper-mentioned variables are sustainable objectives, resource efficiency, and prevented costs.

4.3.1 Prevented Costs

Data indicates that the protective measures implemented within an organization must be economically viable, to remain sustainable in the long run. Even when interviewees could not put a numeric value to indicate the saved costs associated with prevention, they provided nonnumerical examples for the argument, such as how Participant 7 presented an example, that shows how corporate higher-ups see these measures as a required expense, which in turn prevents greater threats: "*In the business world, let's say for example, you would rather pay 10.000 HUF every year (around 25 Euros) than pay 100.000 HUF (around 250 Euros) once the damage is done*". In a similar vein, Participant 6 also mentioned the additional cost to the company's reputation, for why these preventative measures exist: "*If word got out that our system is not secure, no one would do business with us*". Furthermore, Participant 5 indicated that in cases where the damage is severe, it can halt operational activities or cause systematic damage. "*If the database gets breached, anyone whose data was stored there would be compromised. This means that we would essentially have to rebuild the system so that it won't fall for the same reason again. Of course, these would halt any other activity and would take priority instead*".

4.3.2 Sustainable Objectives

The participants listed goals regarding sustainability that are adopted by the top management. Some of the first-order examples include a statement from Participant 1: "*We have so-called OKRs and these OKRs are the indication of the objective key results, and basically these key results always contain some part of sustainability. Usually, we have up to five key results. The first two or three are mainly business related and we have the last two which are a mixture of security and sustainability key results*". As described by the participant, OKRs function similarly to KPIs, with the main difference being that KPIs are often associated with numeric values, while OKRs are centered around achieving a certain goal. "*OKRs are very much similar but not so much focusing on numbers, but rather achieving something*". A different sustainable objective was provided by Participant 5, who said the following: "*We follow the EU Horizon initiative, but to give you specifics, we are mostly focused on promoting healthy competition for the industry we are in and combating climate change of course*". Other organizational intentions included waste reduction initiatives stated by Participant 4: "*Our main goal is to reduce our environmental footprint so that we put less thrash into nature*" These statements highlight a healthy mixture of different goals ranging from the well-known and widely adopted waste reduction to more specific initiatives such as the EU Horizon program.

4.3.3 Resource Efficiency

The last identified data group within sustainable performance was resource efficiency. Participants revealed practices that prioritize optimal resource utilization. The function of these practices can be seen as a complimentary element of cost and waste reduction, due to the limited usage of organizational capital and material. These attributes can be found in Participant 7's statement: "*We do our best to avoid traditional processes where we can. We would rather do online documents instead of using paper, we also prefer online work or meetings, which also reduces transportation*". By switching from traditional to digital processes, the company manages to reduce resources such as time, costs, or raw materials, which could be allocated elsewhere. Participant 7's statement continues with: "*If we did not have this digital infrastructure, I would imagine we would use more classical solutions to achieve the same results, but those would require more time and resources*". A different way to approach resource savings was found in a statement made by Participant 1: *"...In general sustainable development means for the company to be able to produce software that can be used for a long time so considering the cost and environment options. In our case, this mainly means at the moment that we choose those coding languages or those data centers that provide all these services*". Opting for a long-term solution, which favors sustainable usage is a way for the organization to lessen its impact on the environment. On the contrary, Participant 5 reported that the organization utilizes a circular economy, with the prime objective being environmental protection and recycling. "*In our company, we use a circular structure, where our output gets recycled. It makes it easier on us to need less input this way, but this is our way of protecting the environment*".

4.4 Connection Between Variables

This section is meant to represent the results that indicate the link between variables previously described in section 4. (Cybersecurity Threats, Training and Prevention, and Sustainable Performance). This section contains information that relates to the relationships between (1) Cybersecurity Threats and Preventative Measures and (2) Preventative Measures and Sustainable Performance.

4.4.1 Cybersecurity Threats leading to Preventative Measures

The examined variables Training and Prevention are connected to cybersecurity threats due to the primary goal of blocking or minimizing the possibility of cyber-related risks. As indicated by a statement from Participant 6 *"The security procedures and the training we do are a response to the attacks we might face. We actively want to prevent these attacks from happening"* Another statement by Participant 1 indicated the value protection aspect of preventative measures, by stating the following "*I would say on one side there exists danger, and on the other, we have the assets of the company. It should be a simple process to protect your valuables, but in 2024 you have your most important things in your computer, so we use cybersecurity as a way to protect our assets*". These examples showcase the causal relationship between the variables, where the risk and danger presented by cybersecurity threats warrant the use of protective and safety measures in the workplace, such as the use of firewalls, or the implementation of training.

4.4.2 Preventative Measures and Sustainable Performance

This section is meant to emphasize the importance of preventative measures and how they contribute to resource reduction. As stated, in section 4.3.3, the shift from traditional organizational processes to digital ones is enabled by the cybersecurity measures in place. These new practices that are handled in a digital environment require less traditional resources, which in turn leaves the organization with more capital. This is described by the statement for Participant 7, which follows their claim from 4.3.3 "*When we have online meetings for example, we can save time and transportation costs, we use emails instead of printing more paper, these are the things we can spare when we go online*". How cybersecurity practices enable this digital shift is shown in the statement of Participant 6, who said the following "*The digital space around us has to be safe and secure for everyday use, otherwise there would be no work done*". The additional knowledge and safety net provided by cybersecurity practices enables and contributes to a safe and digital working environment.

5. DISCUSSION, LIMITATIONS & FUTURE RESEARCH

5.1 Discussion

The study investigated the relationship between cybersecurity training and its effect on organizations achieving sustainable goals. The findings regarding said relationship, which is based on results extracted from the semi-structured interviews, are summarized below.

At the first level, we have cyberattacks and cyber risks. These variables represent the important initial factor, which leads to cybersecurity practices. The research identified two different types of main digital threats based on origin. External concerns are threats that emerge outside the organization and aim to penetrate the defensive system in place. Examples include phishing attacks, ransomware attacks, and data breaches. On the other hand, internal concerns arise from within the organization and result in potential vulnerability points, which can be taken advantage of. Examples of internal concerns include human error, lack of knowledge, or a weak defensive system. This categorization of technological threats is in line with the findings of Cains (2018), who argued that

cyber-related risks can be caused by both systematic failures as well as human error. If companies aim to negate or reduce the impact of these attacks, that leads to the implementation of safety and security measures (Agrafiotis et al., 2018).

The second factor is the upper-mentioned preventative measures, which aim to make the technological environment a safer space. There are a variety of practices that fall under this category, but the most important one in the context of the study is cybersecurity training and its outcomes. Organizations implement cybersecurity training to enhance the knowledge and skills of the employees, and to reduce the likelihood of detrimental human error that could result in technological complications. The implementation of said training benefits the company as well as the employees who partake in the education. There are similarities between the conceptualized cybersecurity training shown in the literature review, meaning that both variables aim to achieve technological security by improving employee competency (Tsohou et al. 2015; Whitman et al., 2008). However, the way these education methods are implemented differs in approach. Although awareness programs are a common way for organizations to implement said training, real-life examples also offer different approaches such as simulated cyberattacks, that aim to test the employees in a real-world environment while producing first-hand experience.

Another important finding regarding training is that it also contributes towards cost savings by cost avoidance. By reducing the likelihood and impact of potential cybersecurity threats, organizations can avoid the costs associated with a successful cyberattack. This positive result supports the organization's sustainable performance, which transitions into the important factor of sustainability. The last crucial point of this research is the notion of sustainability, which encapsulates two significant factors, sustainability goals and resource management. Following up on the previous paragraph, with the notion that training and preventative measures applied by the organization contribute towards efficient resource utilization. By switching from traditional operational activities to digital processes, organizations can reduce the time, cost, and material associated with traditional processes. This shift and the saving of resources are enabled by the technological safety measures already in place. Since the operations of the organization require fewer resources in terms of time, costs, or material, it results in an efficient utilization of resources. Lastly, the resources saved thanks to digital measures can be used to further enhance the capabilities of the organization towards achieving their sustainability goals. Said objectives aim to reduce the organization's environmental impact while promoting sustainable measures. The cost avoidance aspect of the preventative measures discussed earlier already qualifies as a solid reason for companies to adopt sustainability goals according to Vinichenko (2015), who lists sustainable economic growth, cost reduction, and changing customer preferences among the incentives to adopt sustainable development goals at an organizational level. The study indicates that preventative technological measures such as training positively contribute towards the attainment of sustainability objectives through the efficient use of resources and cost avoidance aspects associated with cybersecurity practices.

Although there is not a direct relationship between cybersecurity training and sustainable goals, the preventative measures, to which cybersecurity training belongs, contribute towards sustainable performance via efficient resource management and the reduction of costs associated with successful cyberattacks. This cost reduction aspect can be considered as a sustainable goal itself, and a reason for organizations to implement sustainable objectives. However, this link is fueled by the causal relationship between technological threats and the implementation of cybersecurity prevention methods.

5.2 Theoretical Contribution

The first theoretical contribution towards established studies is that cybersecurity training does contribute to the overall technological safety system of the company. This is in line with the findings of Tsohou (2015) and Whitman (2008), who argue about the beneficial aspects of implemented training and awareness programs. By adopting preventative measures such as cyber security training, organizations actively lower the potential for a technological vulnerability to occur, while boosting the capabilities of the employees. Hence organizations should widely adopt similar practices for safety purposes. By categorizing cybersecurity threats into two segments, the research aligns the distribution with previous findings and makes a distinction between the dangers faced by organizations. As highlighted earlier, the core difference between external and internal cybersecurity concerns identified through the data lies in the origin of said concerns. External concerns center around attacks that originate from outside the organization intending to penetrate, cause harm, or illegally access an existing system. Based on the findings, these attacks can materialize in the form of data breaches, where the information system of the company gets compromised, which often results in data theft. On the other hand, internal concerns are issues that can cause harm, that are a direct result of poor or incorrect practices within the organization. The lack of or improper execution of practices can lead to technological vulnerabilities, which can be exposed by wrongdoers.

Furthermore, the data collected from the research corresponds to the discovery of Weishäupl (2015), with the supported notion that cybersecurity attacks and digital threats are ever-evolving threats that can disrupt daily operations and existing systems within an organization. By examining real-world cybersecurity threats the data collected through semi-structured interviews contributes to the pre-existing studies. The practical examples present a variety of digital threats that result in harm to the organization. These can range from single-instance scams that participants experience in their day-to-day lives or larger-scale attacks, such as the upper-mentioned security breach.

Regardless of origin, cybersecurity threats cause harm to the organization. To evade said attacks, organizations implement security and preventative measures. These measures range from educational training such as cybersecurity training that reduces the potential risk by enhancing employee competency to more traditional security measures such as firewalls and security codes. The reason why safety measures are used in the business landscape is to prevent cybersecurity risks from happening. This reason coincides with the findings of Hossain (2023), who argued that technology-related harm should be fought against with protective measures.

The last contribution to prior research is the addition to the human capital theory (Jovanovic, 1995). Given that human capital theory positively correlates favorable decision-making outcomes to the time investment into a certain skill, this assumption can explain the positive outcomes of cybersecurity or awareness trainings. By participating in cybersecurity education programs, attendees devoted time and effort to strengthening their technological consciousness. This dedication transforms into knowledge, which in turn enhances employees' capability to handle cybersecurity threats. Since the positive payoffs of the training are a direct result of participation and time investment, this phenomenon ties back to the human capital theory. The examined results, which further highlight the positive relationship between cybersecurity training and technological awareness and reduced risk, demonstrate a real-world application of the human capital theory.

Based on the results and qualitative data analysis a conceptual model can be drawn up, which is showcased in Figure 5.2.1. Additionally, the larger data structure can be found in the appendix under Figure 8.1. Based on the conceptual model, the following propositions can be formulated to answer the initial research question. (1) The sum of external and internal technological concerns can be represented by cybersecurity threats, which influence the existence of preventative measures and training in an organization. As highlighted earlier, these preventative measures aim to reduce the effectiveness of the previously mentioned threats in an organizational setting by applying a variety of safety precautions. (2) The preventative measures and training results in sustainable performance, by reducing the resources and costs associated with successful cybersecurity threats. (3) The cost savings from the preventative measures not only affect sustainable performance but also act as a sustainable objective itself. (4) Having additional resources within an organization contributes to achieving sustainable objectives by providing more resources for the organization to work with. In summary, the outcomes from the preventative measures positively impact the organization's ability to pursue its sustainability objectives.

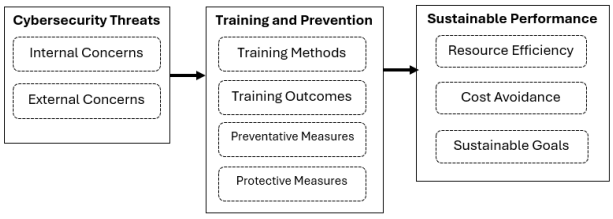


Figure 5.2.1 – Proposed conceptual model on how cybersecurity training impacts sustainable performance

5.3 Practical Implications

The practical implications of this study follow the perception that cybersecurity and other preventative measures such as awareness training bring additional benefits to the organization besides combating technological threats. With the added advantage of cost reduction and assistance in delivering sustainable performance, cybersecurity training can contribute to more areas that enhance organizational performance. This preparedness also correlates with the resilience of the organization towards technological threads.

Following these findings, with the pre-established notion of growing cybersecurity challenges around the world, organizations that operate within a digital environment should consider investing resources into cybersecurity prevention and training, given the potential return and safety features. Under the assumption that prevention and training also contribute to sustainable performance; by applying these practices, organizations can also embrace the adoption of digital processes, which reduce the consumption of resources associated with traditional activities like time or raw materials. Real-world examples of this showcase standardized training for employees, which can be seen as outdated or insufficient. Tailor-made training courses that cater to specific roles within the organization should address this issue, by focusing on the specific needs of different employees.

The implementation of this training should be a universal practice for every employee, meaning that each worker employed by the company should receive standard awareness training that informs people about the potential dangers associated with the digital environment and provides guidance on how to handle certain situations. Moreover, personnel who are more involved with technology should receive additional training that features first-hand experience, tests, and evaluation, since these employees present a significantly higher risk factor than those who are less involved with complex technological processes.

5.4 Limitations

The most noticeable limitations of this study stem from the interview process and the corresponding interview participants. The finite time provided for the research and the data collection process resulted in a lower number of willing respondents than expected when formulating the study. It is also worth pointing out the researcher's lack of prior experience conducting qualitative research.

Additionally, most participants speak English as a second language and often required clarification or examples towards some questions asked during the interview. This might also impact their ability to properly express themselves or limit their vocabulary due to English being a secondary language for them.

Moreover, many participants left a comment, saying that they previously did not believe in the existence of a link between cybersecurity and sustainability, only with the help of the questionnaire they thought such a thing would exist. This might indicate that the questions or the environment of conducting research might have influenced their given responses. However, this can also be a testament to the effectiveness of the questionnaire.

The last limiting factor could be attributed to the fact that the examined variables, namely cybersecurity training and sustainability practices were already present in the environment the interview participants work in. Under opposite circumstances, where the presence of one variable is not as dominant, or in cases where one variable is missing the results might differ significantly.

5.5 Future Research

When conducting research in a similar field, the researcher should be mindful that human participants might not be familiar with the connection between cybersecurity and sustainability practices. Moreover, as mentioned in the previous section, the simultaneous existence of variables might not be present in real-life organizations, so any research done in a similar vein should consider industries where said variables can be found.

Additionally, based on the interviews, investigating the effect of other organizational variables and how they interact with cybersecurity and sustainability practices could present an opportunity for academic contribution. Variables such as culture, strategy, or leadership could be among the elements worth examining.

Lastly, to address the previously mentioned limitations regarding this paper, future research should follow a research plan that is tailored to the local language. This way future participants have a better understanding of the questions and are not limited by their foreign language skills. Another option would be to have translated research questions and guidelines to follow in this regard or to have a translator present to reduce the language barrier between interviewer and interviewee.

6. CONCLUSION

This study investigated the relationship between two organizational variables, associated with twin transition, namely, cybersecurity training and sustainability goals, to answer the question:

"How does the implementation of cybersecurity training contribute towards organizations achieving sustainable development goals"

By conducting semi-structured interviews and adopting a qualitative research method, the results indicated that cybersecurity and other technological threats lead to the existence of preventive measures, which include employee training. Said measures are in place to defend the company from the dangers associated with digital presence, such as phishing or ransomware attacks. This training contributes towards enhanced knowledge in the field of technology, while also helping the organization by avoiding costs associated with cyberattacks. Furthermore, the adopted preventative measures influence the organization's ability to perform more sustainably, by using fewer resources and saving capital. Those resources gained from sustainable performance can be utilized to realize organizations' sustainable objectives. Although the link between cybersecurity training and sustainable goals is not a direct one, cybersecurity prevention measures do however offer additional benefits related to sustainable performance.

7. REFERENCES

Agrafiotis, I., Nurse, J. R. C., Goldsmith, M., Creese, S., & Upton, D. (2018). A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate. Journal of Cybersecurity, 4(1). https://doi.org/10.1093/cybsec/tyy006

Ahola, M. (2022b, June 17). The Role of Human Error in Successful Cyber Security Breaches. usecure. https://blog.usecure.io/the-role-of-human-error-in-successful-cyber-security-breaches

Becker, G. S. (1962). Investment in Human Capital: A Theoretical analysis. Journal of Political Economy, 70(5, Part 2), 9–49. https://doi.org/10.1086/258724

Beuran R., Pham C., Tang D., Chinen K., Tan Y. and Shinoda Y. (2017). CyTrONE: An Integrated Cybersecurity Training Framework.In Proceedings of the 3rd International Conference on Information Systems Security and PrivacyISBN 978-989-758-209-7, pages 157-166

Boddy, C.R. (2016), "Sample size for qualitative research", Qualitative Market Research, Vol. 19 No. 4, pp. 426-432. https://doi.org/10.1108/QMR-06-2016-0053

Boeije HR. Analysis in Qualitative Research. London (UK): Sage Publications; 2009

Braun V, Clarke V. Using thematic analysis in psychology. Qualitative Research in Psychology. 2006;3:77-101

Brinkmann, S. (2023b). The line as a root metaphor for qualitative psychology. In Routledge eBooks (pp. 26–36). https://doi.org/10.4324/9781003132721-4

Chandra, A., & Snowe, M. J. (2020b). A taxonomy of cybercrime: Theory and design. International Journal of Accounting Information Systems, 38, 100467. https://doi.org/10.1016/j.accinf.2020.100467

Cains, M. G., Flora, L., Taber, D., King, Z. M., & Henshel, D. S. (2021). Defining Cyber Security and Cyber Security Risk within a Multidisciplinary Context using Expert Elicitation. *Risk Analysis*, *42*(8), 1643–1669. https://doi.org/10.1111/risa.13687

Christmann, A., Crome, C., Graf-Drasch, V., Oberländer, A. M., & Schmidt, L. (2024). The Twin Transformation Butterfly. Business & Information Systems Engineering. https://doi.org/10.1007/s12599-023-00847-2

Conceptual model of Visual Analytics for hands-on cybersecurity training. (2021, August 1). IEEE Journals & Magazine | IEEE Xplore. https://ieeexplore.ieee.org/abstract/document/9018081CyberPeace Institute (2022) "Cyber Peace and the United Nations (UN) Sustainable Development Goals (SDGs)", Blog.

Czernek-Marszałek, K., & McCabe, S. (2024). Sampling in qualitative interview research: criteria, considerations and guidelines for success. Annals of Tourism Research, 103711. https://doi.org/10.1016/j.annals.2023.103711

Daly, Herman E (2006) "Sustainable Development—Definitions, Principles, Policies", in The Future of Sustainability. Dordrecht, Springer Netherlands.

Gioia, D. A., & Pitre, E. (1990). Multiparadigm perspectives on theory building. the Academy of Management Review, 15(4), 584–602. https://doi.org/10.5465/amr.1990.4310758

Gioia, D. A., Corley, K. G., & Hamilton, A. L. (2012). Seeking qualitative rigor in inductive research. Organizational Research Methods, 16(1), 15–31. https://doi.org/10.1177/1094428112452151

He, W., & Zhang, Z. (2019b). Enterprise cybersecurity training and awareness programs: Recommendations for success. Journal of Organizational Computing and Electronic Commerce, 29(4), 249–257. https://doi.org/10.1080/10919392.2019.1611528

Hossain, N. U. I., Rahman, S., & Liza, S. A. (2023). Cyber-susiliency index: A comprehensive resiliency-sustainability-cybersecurity index for healthcare supply chain networks. Decision Analytics Journal, 9, 100319. https://doi.org/10.1016/j.dajour.2023.100319

How COVID-19 has pushed companies over the technology tipping point—and transformed business forever. (2020, October 5). McKinsey & Company. https://www.mckinsey.com/capabilities/strategy-and-corporate-finance/our-insights/how-covid-19-has-pushed-companies-over-the-technology-tipping-point-and-transformed-business-forever

Cost of a data breach 2023 | IBM.(n.d.).https://www.ibm.com/reports/data-breach

Jibi M. B., Neethu G., Anju J. P., (2019). Cyber attacks and its different types. International Research Journal of Engineering and Technology (IRJET) Volume: 06 Issue: 03

Jovanovic, B., & Nyarko, Y. (1995). The transfer of human capital. Journal of Economic Dynamics & Control, 19(5–7), 1033–1064. https://doi.org/10.1016/0165-1889(94)00818-3

Kalogiannidis, Stavros, Maria Paschalidou, Dimitrios Kalfas, and Fotios Chatzitheodoridis (2023) "Relationship between Cyber Security and Civil Protection in the Greek Reality", Appl Sci. 13(4): 2607

Katekovi, M. and Mantere, S.(2010) 'TWO STRATEGIES FOR INDUCTIVE REASONING IN ORGANIZATIONAL RESEARCH' , Academy of Management Review, Vol. 35, No. 2

KIM PARKER, HOROWITZ, J. M., & MINKIN, R. (2022). COVID-19 Pandemic Continues To Reshape Work in America.

Kluczek, Aldona, Bartlomiej Gladysz, Aleksander Buczacki, Krzysztof Krystosiak, Krzysztof Ejsmont, and Erika Palmer (2023)"Aligning sustainable development goals with Industry 4.0 for the design of business model for printing and packaging companies",*Packag Technol Sci. 36(4): 307–25*

Koetsier, J. (2022b, April 14). E-Commerce jumped 55% during Covid to hit $1.7 trillion. Forbes. https://www.forbes.com/sites/johnkoetsier/2022/03/15/pandemic-digital-spend-17-trillion/

Kücükgül, E., Cerin, P., & Liu, Y. (2022). Enhancing the value of corporate sustainability: An approach for aligning multiple Liamputtong, P. (2009b). Qualitative data analysis: conceptual and practical considerations. Health Promotion Journal of Australia, 20(2), 133–139. https://doi.org/10.1071/he09133

Lukas Stratmann, Gerrit Hoeborn (2022). Twin-Transition: Digitalisierung und Nachhaltigkeit Hand in Hand | Digitalization and Sustainability Hand in Hand

MacLeod, W. B. (2016). Human capital: Linking behavior to rational choice via dual process theory. Labour Economics, 41, 20–31. https://doi.org/10.1016/j.labeco.2016.05.019

Mincer, J. (1958). Investment in human capital and personal income distribution. Journal of Political Economy, 66(4), 281–302. https://doi.org/10.1086/258055

Nakhle, P., Stamos, I., Proietti, P., & Siragusa, A. (2024). Environmental monitoring in European regions using the sustainable development goals (SDG) framework. Environmental and Sustainability Indicators, 21, 100332. https://doi.org/10.1016/j.indic.2023.100332

R. J. Whittingham, Hélène Gaudin, The rising role of cybersecurity in ESG and how companies are taking action. (n.d.-b). ERM. https://www.sustainability.com/thinking/the-rising-role-of-cybersecurity-in-esg-and-how-companies-are-taking-action/

SDGs guides on reporting. Journal of Cleaner Production, 333, 130005. https://doi.org/10.1016/j.jclepro.2021.130005

Sulich, A., Rutkowska, M., Krawczyk-Jezierska, A., Jezierski, J., & Zema, T. (2021). Cybersecurity and sustainable development. Procedia Computer Science, 192, 20–28. https://doi.org/10.1016/j.procs.2021.08.003

Sulich, A., Zema, T., & Kulhanek, L. (2023). Towards a Secure Future: A bibliometric analysis of the relations between cybersecurity and sustainable development. Procedia Computer Science, 225, 1448–1457. https://doi.org/10.1016/j.procs.2023.10.133

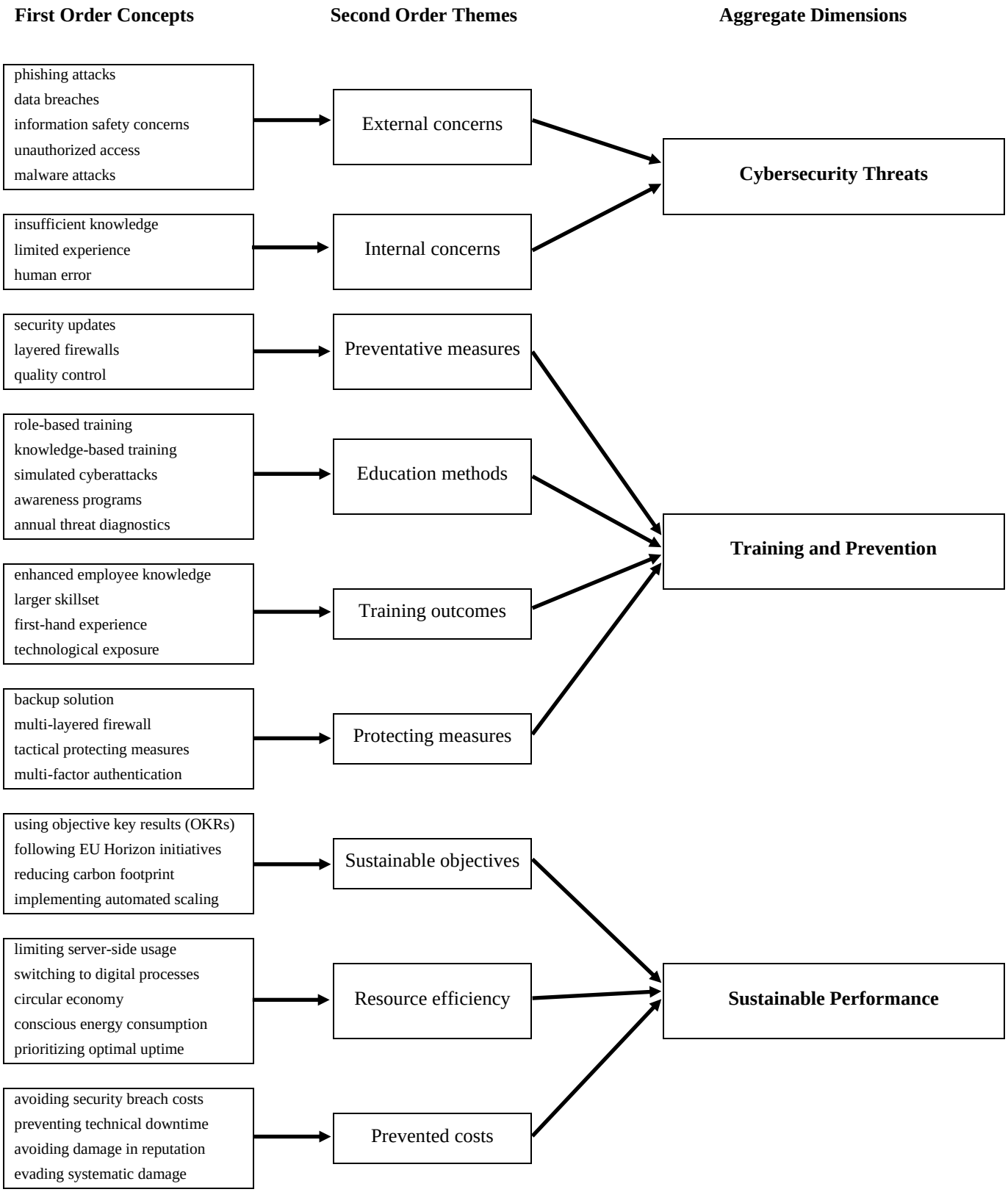
Verizon, “2022 Data Breach Investigations Report,” 2022.

Wall, D.S. Introduction: Cybercrime and the Internet. In Crime and the Internet; Wall, D.S., Ed.; Routledge: New York, NY, USA, 2001

Weishäupl, Eva ; Yasasin, Emrah ; Schryen, Guido (2015) | Universität Regensburg. A Multi-Theoretical Literature Review on Information Security Investments using the Resource-Based View and the Organizational Learning Theory

8. APPENDIX

8.1 Initial Data Structure



8.2 Interview Guidelines

Introductory questions

1. Before we begin, can you Introduce yourself please?

2. Could you briefly describe your field of work?

3. Can you present your company/organisation - your values

Interview questions

1. What does sustainable development mean to you, or your company?
    a. Do you think your role has additional responsibilities towards sustainable development? If yes, or no, why?

2. How does your company define Sustainable Development Goals?
    a. What are the methods, or practices used to realise said goals?
    b. What are the measures that indicate success in this context?

3. What are your thoughts on the role of digitalization in addressing sustainability challenges?

4. Why do you think cybersecurity is important/unimportant in the current landscape?

5. How do you prepare for cyberattacks within the company? (does that include training)
    a. Did you facilitate, or participate in any form of cybersecurity training, if so, can you tell me more about it?

6. What are the components of your cybersecurity program?
    a. Do you think your role in the company warrants said cybersecurity training? If yes, or no, why?

7. From your experience, why do companies implement cybersecurity training?

8. How do you perceive the economic benefits of investing in cybersecurity training within an organization?

9. How do you perceive the relationship between effective cybersecurity training and potential cost savings or revenue generation within organizations?

10. In what ways do you think improved cybersecurity practices contribute to sustainable goals?

Closing questions

1. In your opinion, what is the connection between your organization's environmental sustainability goals and cybersecurity training programs?
    a. How does cybersecurity training contribute towards those goals? (if it does not contribute, why?)

2. Could you give examples of cybersecurity practices negatively or positively impacting sustainability efforts within organizations?

3. What opportunities present themselves in the field of sustainability when companies implement cybersecurity training/practices?

4. After our discussion, do you think that cybersecurity, and cybersecurity training in particular, influences sustainable goals? If yes, or no, why?

5. Is there anything else I did not ask about, that you would like me to know?