The Classification and Impact of Cyber Attacks Targeting Critical Service Providers

Josefin Andersson and Elias Seid
Department of Computer and Systems Sciences, Stockholm University, Sweden
{*josefin.andersson, elias.seid*}*@dsv.su.se*

Keywords: Cybersecurity, IT-Incidents, Societal Safety, Critical Infrastructure, Essential Services, NIS-Directive, Impact Assessment, Cyberattack.

Abstract: Over the past few decades, technological solutions have become increasingly crucial for providers of societal services. Though increased productivity is advantageous, it also exposes people to the vulnerability of cyber-attacks that aim to disrupt their systems and networks. While security agents issue new indicators and patches to address breaches, the ever-changing nature of these indicators renders security solutions to cyber-attacks potentially obsolete. Therefore, defending cyber-attacks requires a continuous and ongoing process. A thorough analysis of the impact of cyber security on the cyberinfrastructure and functionality of critical service providers is lacking. Conducting an analysis of cyberattacks and their impact on both digital and non-digital domains is crucial for obtaining a thorough awareness. The Swedish Civil Contingencies Agency (MSB) receives reports of IT incidents from Service Providers and Government Agencies that are within the jurisdiction of the European Union. This study analyses IT incidents reported to MSB to enhance knowledge of cyber-attacks and their impact on vital service providers. It evaluates the impact of cyberattacks on infrastructure, organisations, and society. The objective is to analyse the impact of cyberattacks on the cyberinfrastructure of vital service providers and their implications for organisations and society. Moreover, this paper categorised the internal and external impact of cyber attacks, demonstrating the broad cyber threat landscape and vulnerability of crucial service providers in Sweden.

1 INTRODUCTION

Over the past decade, various sectors within society have experienced a rapid process of digitalization. One significant trend involves the migration of crucial information resources and organisational procedures from physical to digital platforms. The implementation of novel sociotechnical solutions has brought about numerous advantages by significantly enhancing operational efficiency in both corporate and governmental organisations, thereby altering the landscape of information and process management. However, it has also presented novel challenges. The growing dependence on systems and networks has resulted in heightened susceptibility of critical service providers, such as government agencies and healthcare organisations, to incidents that impact their operations (Urbach and Röglinger et al., 2018).

Cybersecurity incidents that impact the cyberinfrastructure, encompassing the network and system resources of significant service providers, have the potential to significantly disrupt crucial digital operations. Consequently, this disruption indirectly hampers the organization's capacity to effectively deliver services to its stakeholders. In addition to the general public, various other organisations are also involved. This prompts inquiries into the extent to which cyberattacks can inflict damage on organisational systems and networks, as well as indirectly impacting organisational functions and society as a whole [1]

The occurrence of cyberattacks, such as the one committed against the Kalix municipality in Sweden in December 2021, resulted in the unavailability of numerous municipal services due to the encryption of critical assets through ransomware.

In contemporary times, the emergence of cutting-edge technological advancements in domains such as Artificial Intelligence, Internet of Things, and cloud computing has given rise to novel vulnerabilities and subsequently posed significant cybersecurity challenges. The significance of understanding the cyber threat landscape encountered by crucial service

[1] https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022

Andersson, J. and Seid, E.
The Classification and Impact of Cyber Attacks Targeting Critical Service Providers.
DOI: 10.5220/0012374500003648

In *Proceedings of the 10th International Conference on Information Systems Security and Privacy (ICISSP 2024)*, pages 137-145
ISBN: 978-989-758-683-5; ISSN: 2184-4356

providers and the potential consequences of attacks against them has been increased by these advancements [2]

Insufficient study has been conducted to look at the impact of cyberattacks on major service providers. Moreover, there is inadequate scrutiny regarding the extent of the impact these attacks have had on the cyberinfrastructure of organisations, as well as the frequency at which incidents result in adverse consequences beyond the digital domain.

The absence of research focused on the characterization and consequences of malicious activity directed at significant service providers can be considered problematic from various viewpoints. According to (Plachkinova and Vo et al., 2023) and(Paté-Cornell and Kuypers et al., 2023), it has been argued that this trend may have implications for organisations' capacity to effectively assess risk. This is due to a limited understanding of the probability and characteristics of potential attacks. (Caldarulo et al., 2022) and (Agrafiotis et al., 2018) points out the lack of research on the adverse effects of cyber attacks, which hinders researchers' capacity to identify the organisational and societal consequences of such malicious activities.

Objective of this study: This paper investigates the defining characteristics of cyber attacks that specifically target significant service providers in Sweden. It also explores the extent to which these incidents are capable of impacting both the targeted organisations and society as a whole, encompassing both the digital realm and its broader implications. This study analyses cyber security incident reports submitted to MSB to enhance understanding of cyberattacks and their impact on critical service providers in Sweden. The study aims to address the following research questions (RQs), and the research questions are answered based on the cyber security incident reports provided to MSB.

- RQ1. What is the impact of reported cyberattack incidents on the organisational, social, and cyber aspects of critical service providers' cyberinfrastructure?

The remainder of this paper is organized as follows. Section 2 presents the research baseline for our work, while Section 3 presents methodology and a case study. In section 4 we provide results, while section 5 deals with discussions. Section 6 concludes and discusses future work.

2 RESEARCH BASELINE

2.1 Digitising Critical Service Providers

The convergence of physical and digital dimensions through digitalization has led to increased speed and connectivity for society. (Urbach and Röglinger et al., 2018) argue that technology integration has increased volatility, uncertainty, complexity, and ambiguity in social contexts. (Ulrich Beck et al., 1992) argued that modern society has become a risk society due to increased complexity, which drives comprehensive risk management. (Arjen Boin et al., 2018), inspired by Beck and interested in the impact of digitalization on societies' ability to contain incidents, proposed that digitalization and globalisation contributed to the transboundary crisis.

The need for specific measures has evolved as more information assets and processes transition to technology (Markoupolou and Papakonstantinou et al., 2021; Osei-Kyei et al., 2021). This development coincides with the securitization of cyberspace, emphasising cyber threats as a matter of internal and national security (Hansen and Nissembaum et al., 2009). The study conducted by (Høyland et al. (2018) emphasises the increasing significance of cyber threats to societal services and infrastructures. These threats result in more complex and uncertain risks, which require interdisciplinary solutions. In terms of academia, the disciplines of ”societal safety” and ”societal security” have combined, advocating for a ”all-hazards” strategy. Sweden has traditionally adopted a comprehensive approach in its policies, considering all types of hazards. MSB, includes adversarial hazards in its assessments of national risks (Pursianien et al., 2018).

As the EU emphasises cyber threats to internal market stability, the merger becomes more apparent (Calderaro and Blumfelde et al., 2022). According to (Whyte et al.,2021), the EU's cyber governance understanding is influenced by real situations more than other authorities. Whyte et al. (2021) list 12 events that could affect social and economic stability. The EU Cyber Security Act defines cybersecurity as protecting IT resources and incident victims. EU regulations are raising cybersecurity standards for key actors as digital integration blurs service provider lines (Papakonstantinou et al., 2022).

2.2 The Classification of Impact in Cyber Physical-Systems

According to Syafrizal et al. (2021), the rapid pace of cyber development has led to a lack of consensus

[2] https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022

on cyberattacks and their consequences. This study adopts Derbyshire et al. (2018)'s definition of a cyberattack, which includes a wide range of ”offensive actions” that affect an organization's cyber infrastructure. DDoS attacks and cyber-exploitation, which involves unauthorised information gathering, are offensive actions (Harry and Gallagher et al., 2018).

Cyberattacks on cyberinfrastructure potentially target processes, hardware, and users. Syntax (malware) and semantic (social engineering) cyberattacks can access targeted cyber infrastructure (Syafrizal et al., 2021; Harry and Gallagher, 2018). Derbyshire et al. (2018) define ”offensive action” as social and non-digital actions, including physical hardware targeting.

According to (Mancuso et al., 2014), cyberattack frameworks typically include five components: **goal**, **attack-source**, **target**, **attack vector**, and **impact**. The authors identify three dimensions of these components: **adversarial**, **methodological**, and **operational**, to differentiate their qualities better.

Adversarial refers to the threat actor and their attack strategy and objectives. Threat actors use methodological methods to achieve their goals. Finally, operational dimension refers to cyberattack impact on targeted infrastructure. Operational cyberinfrastructure impacts the targeted system, network or information assets (Mancuso et al., 2014).

The AVOIDIT cyberattack taxonomy, developed by Simmons et al. in 2009, is a widely recognised and frequently referenced framework in academic literature. One could argue that this framework primarily focuses on the operational aspect of cyberattacks. Simmons et al., 2009 present a classification framework comprising four classifiers to classify attacks. The following are the classifiers: 1) **Attack Vector**, 2) **Operational Impact**, 3) **Informational Impact**, and 4) **Attack Target**

Further, a classifier was added to classify incidents by preferred defensive measures. Simmons et al. (2009) define attack vector as the path to access the targeted component, similar to MITRE's ”initial access” definition [3]. Unlike MITRE, AVOIDIT framework focus on exploited vulnerabilities rather than cyberattack tactics and techniques. Simmons et al.'s 2009 operational and informational impact classifiers describe impact.

Operational impact includes ”web compromise,” ”installed malware,” and ”denial of service.” Informational impact classifies how the attack affects cyber infrastructure informational resources. The classifier includes “distortion” and “disclosure” categories. The terms “installed malware” and “disclosure” refer to cyberattacks that use spyware and other methods to steal data. Simmons et al.'s (2009) attack target classifier targets “network” and “user” cyberinfrastructure.

2.3 Organizational and Societal Impact

Cyberspace incidents have had major effects on the real world due to digital convergence. Berg and Kuipers et al. (2022) distinguish cyber-incidents' direct and indirect harm. Direct impact on cyberinfrastructure describes how various activities can allow unauthorised access, modification, or removal of digital resources. Direct impact resembles Simmons et al. (2009)'s operational and informational impact classifiers. Berg and Kuipers et al. (2022) define indirect impact as an incident outside of a digital space. Cyber events have primary and secondary effects (Harry and Gallagher et al., 2018).

Economic and financial impact is important for situations like losing competitive advantage due to sensitive information disclosure or a disruption. (Shevchenko et al., 2023) analyse the average cost of cyber incidents across business sectors to determine the most impactful types. Their cyber risk model (Paté-Cornell and Kuypers et al., 2023) includes financial loss.

Agrafiotis et al. (2018) say harm has evolved with security. The authors suggest that cyber harm science should consider physical and psychological harm to individuals and communities. In order to achieve this, Agrafiotis et al. (2018) identified five main categories: Physical or digital, economic, psychological, reputational, and social. Physical or digital harm includes both individual and cyberinfrastructure damage. Society suffers daily disruptions, national damage, and lower employee morale .

3 METHODOLOGY

The present study employs a survey-based research methodology to achieve the stated objective. Therefore, it is deemed suitable for conducting a study of this nature, which seeks to portray the cyber threat landscape across a significant number of organisations. The present study uses IT-incident reports as the primary data source, which were obtained from MSB . Furthermore, the research was conducted using a secondary dataset consisting of written IT-incident reports. These reports were submitted to MSB by different government agencies and organisations in Sweden. The selection of this dataset adhered to the guidelines specified in the European Union's NIS-directive. The objective of this study is to contribute to the existing body of knowledge by using non-

[3] https://attack.mitre.org/

publicly accessible data that offers a broader scope of coverage compared to alternative sources. Collecting information about IT incidents from significant service providers could bring challenges due to the sensitive nature of the data. Employing this source is advantageous due to the limited availability of information on this topic to the general public. The reporting schemes are uniquely suitable due to their coverage of a significant number of vital service providers. This approach may be limited by the fact that the secondary data used was not collected for this study. This limits the analysis. Conclusions depend on the data quality and format of MSB's IT-incident reports. Another constraint is using reported incidents to analyse the cyber threat landscape, which depends on organisations' reporting choices and methods.

Analysis. The tool provides the ability to analyse both explicit and inferred value. This study employs a directed content analysis approach for analysing inferred meaning. The coding methodology for the reports is pre-established before conducting data analysis, using prior research in the field of cyberattack classification. The classification process will be directed by the semantic interpretation of the report contents, as specified by (Hsieh and Shannon et al., 2005). The use of content analysis is considered suitable for this study owing to the inherent attributes of the data source. The involvement of researchers during the analysis contributes to the observed variations among the questionnaires for IT-incident reports.

The data processing procedure was conducted in four distinct stages. In the initial phase, all IT incidents that occurred between April 1, 2019, and April 1, 2023, were collected, and only the incidents that described malicious events were identified. The remaining individuals were omitted from the dataset. In order to accurately categorise the malicious incidents, the complete reports were thoroughly analysed, encompassing responses to both closed-ended and open-ended inquiries. In the second stage, the IT-incident reports were classified based on the attack vector, operational and informational impact, attack target, and organizational/societal impact.

The findings were then converted into a comparable and measurable format. Incidents that lacked sufficient information to be classified by each classifier were categorised as **unknown**. In the third phase of the data analysis process, the quantities within each category were summarised in order to facilitate frequency comparisons. This was done using Microsoft Excel to organise and analyse data. In the fourth stage, Excel was used to graph and diagram the results. MSB received 1332 IT-incident reports from important service providers between April 2019 and 2023, with 256 from NIS-organizations and 1076 from government agencies. In 254 reports, malicious events were described. Other causes of the remaining incidents included technician and user errors, system failures, natural events, and unknown

4 RESULTS

4.1 Attack Vector

The Attack vector classifier categorises cyberattacks based on the vulnerability exploited or attempted to compromise the organization's cyber infrastructure. The analysis revealed that social engineering was the most prevalent category of reported cyberattacks. Approximately 32% of IT-incident reports describing cyberattacks (81 cases) used social engineering techniques to gain initial access. This category includes **phishing**, **spear phishing**, and other manipulation attempts aimed at deceiving the recipient into taking certain actions.

The large amount of social engineering incidents suggests that deception is a common way to gain access to key service providers. Insufficient capacity was the second most common attack vector, accounting for 28% of reported cyberattacks and 72 cases. This category refers to attacks that exploit cyber infrastructure limitations, such as DDoS attacks. .

Insufficient authentication refers to the use of techniques, such as brute-force attacks, to bypass authentication processes. Meanwhile, the term "Unknown" refers to incidents where the reporting organisations did not provide sufficient details in their description of the event to determine the specific attack method used. Subsequently, there were instances of **inadequate input validation** and **misconfiguration** accounting for 9%, 5%, and 5% of the occurrences, respectively. The "Other" category encompasses reports that describe an attack method that does not fall under any other specified categories. These primarily describe broad vulnerability in systems and code.

According to attack vector usage, social engineering cases increased in April 2019-2020 and 2020-202. Social engineering was used in 44% and 49% of reported malicious incidents during these periods. After that, social engineering became less common, contributing only 15% of reported cyberattacks in 2022-2023. This may suggest that threat actors are using more diverse attack vectors. Instead, targeted organisations are becoming better at defending against these attacks and report them less. By April 2022-2023, capacity limits had become a major attack vector, rising from 20% to 52%.

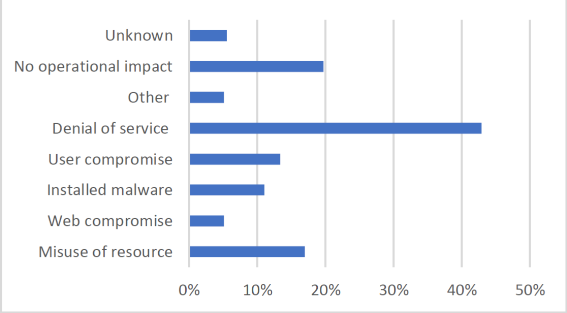

Figure 1: Categories of Operational impact.

4.2 Operational and Informational Impact

The classifiers of Operational and Informational impact have in this study previously been described as forms of direct impact within the cyber infrastructure. Based on the reports, the most common direct impact generated by an attack, looking at both operational and informational consequences, is **the disruption in access to information resources and systems**. As seen in figure 6, cyberattacks resulting in the operational impact of Denial of service has been concluded to account for 43 percent, or 109 cases in total, of reported malicious incidents.

In 17% of incident reports, resource misuse was reported, followed by account hijacks in 13%. Threat actors installing malware in an organization's cyber infrastructure comprise 11% of cyberattacks, which total 28 cases. Website resource compromise incidents make up about 5% of incidents. Unknown and Other made up 6% and 5% of reported cyberattacks. The Other category mostly includes fraud cases. The attacks mostly affect human behaviour and economic loss.

In 44 cases (17%), the attacker's operational impact was classified into multiple categories. On compromised systems, 39% of users install malware. 32% of compromised user accounts were infected with malware. Approximately 20% of DDoS attacks involved operational compromises, with resource misuse being the most prevalent (11 cases).Incident reports often describe availability disruption as an informational impact. About half of malicious activity-related incidents disrupt information and system access. Reports indicate that disruptions resulted in information disclosure in 16% of cases. Information is distorted in about 8% of cases.

Approximately 4% of cases involved mapping and discovering the organization's network and systems structure. In only 1% of cyberattack reports, information assets are permanently lost, making information destruction a rare impact. This may be because companies are preventing permanent data loss.

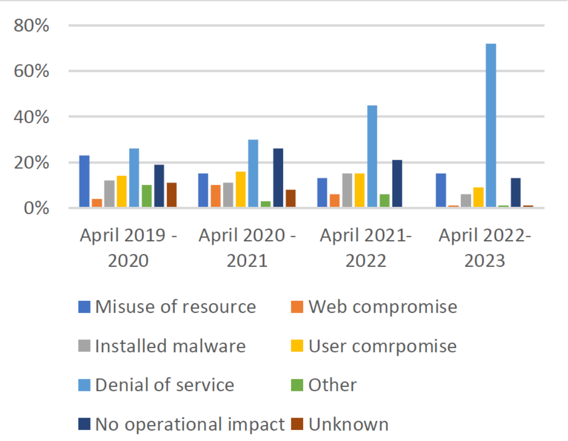

Figure 2: Operational impact.

In contrast to the CIA-triad, most observed cyberattacks compromise availability, while fewer compromise confidentiality and integrity. The IT incident reports may be biassed due to the requirement for NIS organisations to report incidents that disrupt or degrade their operations.

Numerous incidents were found to have no operational or informational impact, according to the analysis. Analysis of reported malicious activity revealed that over 20% of cases had no operational impact on the organization's cyber infrastructure. Additionally, 22% of attacks were reported as having no impact on the organisations' data. Around 15-21% of cyberattacks between April 2019 and 2023 involved IT incidents that did not appear to impact the targeted cyber infrastructure. In April 2022-2023, only 12% of incidents were classified as having no direct impact, according to the study's definition. In cases without direct impact, social engineering and insufficient authentication failed. Authentication vulnerabilities and cognitive biases may increase failure risk. Based on incident reports, this study may help organisations identify failed vector attacks. Out of 109 identified **denial of service attacks**, 94% caused availability disruptions. One malware case had no informational impact, while three had an unknown impact, indicating that the organisation reported a malware infection but not its consequences.

Among installed malware, 67% reported disruption, 29% and 25% reported distortion and disclosure. Due to the low value of informational impact, this study cannot evaluate these attacks beyond their organisational and societal impact. In more IT incident reports, attacks affect information rather than operations. This may be due to cyber infrastructure protection measures that affect information. Denial of service attacks comprised 26% of cyberattacks in April 2019-2021 and 72% in April 2022-2023.

The analysis shows the share has increased proportional and constant since April 2020. Other operational impacts may not show a trend. In the past few years, incidents disrupting information assets and systems have increased from 34% in April 2019-2020 to 69% in April 2022-2023. Denial of Service attacks don't always disrupt. About 3% of reports showed no disruption from a Denial of Service attack. Organisations may have taken precautions to keep targeted data.

4.3 Attack Target

In the study, the fourth classifier identified cyber infrastructure components as targets for malicious activity, including incidents within the reporting organization's supply chain. The most common category of attacks described was targeting software/software systems. In 120 reported incidents, this occurred in 47% of cases. In 96 reports, 38% of all cases involved attacks targeting users. Following this, 26 reported cases involved attacks on network infrastructure. In 7 cases, the targeted cyber infrastructure was classified as Unknown due to insufficient information in the IT-incident report. Figure 13 indicates that 47% of reported cyberattacks targeted websites, while 10% and 8% targeted emails or databases, respectively.

Further analysis revealed that 70% of attacks causing denial of service targeted software/software systems, while 39% targeted websites. Many incidents have not affected internal cyber infrastructure, but had the potential to disrupt external access to website resources. Additionally, 64% were attributed to threat actors targeting processing/network capacity, resulting in DDoS-attacks. About 16% of attacks, or 41 cases, involved organisations indirectly affected by the cyberattack via supply chain links. The organisations were affected due to a supply chain organisation being compromised. In 59% of cases, the incident targeted the organization's software system, while 22% affected a network supplier.

Attacks on various cyber infrastructure components have had a direct impact on various degrees. Out of the attacks targeting users, predominantly using social engineering, 39% have not had any direct impact. Approximately 4% of attacks on software systems directly have not had any direct impact. All reported attacks on network infrastructure components have effectively caused direct impact. there has been a relative increase in attacks targeting software systems as well as relative decrease in attacks targeting users' accounts more specifically.

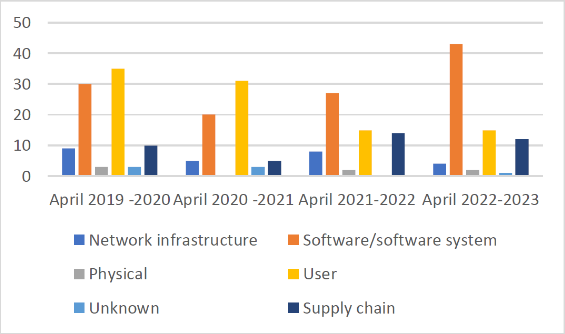

Figure 3: Cyber infrastructure component which have been targeted.

4.4 Organizational and Societal Impact

Finally, investigating the indirect impact of malicious incidents involved determining if IT-incident reports described economic, psychological, reputational, or physical harm to the organisation and wide-ranging disruption with a societal impact. No indirect impact case described no realised consequences beyond the cyber infrastructure, and Unknown case contained no further details. Based on the criteria, many attacks were classified as unknown. Approximately 17% of cyberattacks had an unknown indirect impact, indicating insufficient report detail for conclusions.

Economic was the most common organisational impact description in reports, at 19%. These incidents include disruptions that increased employee workload and cyber infrastructure component replacements. After that, Reputational (12%) and Psychological (8%) were the most common organisational impact categories. Many user compromise incidents had reputational or psychological consequences. About 5%, or 13 cases, had societal impact. None of the incident reports reported physical harm to people. Some reports mentioned a health risk, but none proved it.

No operational or informational impact was reported for 55% of incidents without indirect harm. While the remaining incidents affected the organization's cyber infrastructure, they did not have significant indirect effects. 71% of economic impact incidents targeted software systems, while the same percentage targeted suppliers to the reporting organisation. Moreover, 65% of respondents cited denial of service as an operational impact, while 20% attributed it to resource misuse.

Anyone with a social impact was denied service. Nearly 54% of respondents reported resource misuse and denial-of-service, indicating cyberinfrastructure intrusions caused disruptions, not DDoS attacks. Approximately 71% of respondents reported an attack on an organization's software system. Around 71%

of respondents said the attack affected their organisation via supply chain links, indicating they were not directly targeted.The attack affected the organization's supply chain, but they weren't directly targeted. Incident reports on societal impact often lacked attack vector details, with 62% being unknown. Supply chain incident reports mentioned the same incident and supplier. This suggests that these important service providers' outsourcing and shared suppliers increased the risk of wider disruptions.

5 DISCUSSION

5.1 The Impact Within the Cyberinfrastructure

After analysing Simmons et al.'s (2009) operational and informational impact classifiers, denial-of-service and disruption are the main direct impacts on major service providers' cyberinfrastructure. These attacks have increased during the survey. In many cases, distributed denial-of-service (DDoS) attacks are implicated. Furthermore, many attacks indicate the goal was to disrupt website resources. DDoS attacks and disruptions have been linked to cyberinfrastructure intrusions, resource misuse, and malicious software installation. When comparing the effectiveness of DDoS attacks, 94% caused varying degrees of disruption.

The study does not specify the duration or services most affected by these disruptions. Many denial-of-service attacks involve distributed attacks on website resources, according to previous research. Website outages only affected external access, not employee information. Attacks can also cause DDoS. Social engineering attacks are still common despite a decline. Social engineering and insufficient authentication attacks did not hit major service providers' cyber-infrastructure as severely. As mentioned, organisations' awareness of initial access attempts may explain the trend. Social engineering to illegally access user accounts has decreased, but major service providers still report it as a significant malicious incident. Web compromise was rare compared to resource misuse and denial-of-service attacks. The most common impact reported was disruption, followed by disclosure, and a malicious event at 16%. Service disruptions or degradation outnumbered integrity or confidentiality breaches. Critics of this study may point to bias in organisation incident reporting criteria.

5.2 Implications on Organisations and Society

Researchers claim digitalization has increased the risk of it-incidents cascading beyond digital and organisational boundaries. Organisations rely more on complex systems and supply chains. The study's finding that many incidents indicated the attack had no effect was noteworthy. Over four years, 17% of reported incidents had no direct impact on the organization's cyberinfrastructure. About 20% indicated the incident did not indirectly impact the organisation, while only 6% stated it affected society. An extra 17% lacked sufficient data to classify indirect impacts.

This study shows that many cyber incidents affecting the organization's infrastructure have no reported impact on the organisation or stakeholders, despite the impression of vulnerable service providers. This may have multiple causes. Important service providers reduce direct and indirect attack damage. Key services or society may be strong enough to prevent many reported incidents from damaging. Our analysis showed few incidents that destroyed information assets, suggesting threat actors do not target them and critical service providers can prevent this. These findings do not prove cyberattacks are ineffective, but they challenge the idea that critical service providers and society are overly vulnerable to malicious attacks.

This study does not measure impact, but some incidents may have significant economic, reputational, or societal effects. Supply chain and denial-of-service attacks often had organisational and societal effects. Complex supply chains make incidents harder to manage, according to study. Threats to a critical service provider's supplier can affect values beyond cyberspace, making prevention difficult. Results show that incident reports about social impact often involve the same suppliers. Key service providers using the same suppliers are hazardous.

5.3 Threats to Validity

Access to major service provider cyber threat landscape data improved the study's validity, generalizability, and credibility. Although not all critical service providers must report incidents to MSB, the study's findings may be questioned. Different incident reporting and information inclusion criteria between government agencies and NIS organisations affect results. NIS organisations, unlike government agencies, do not need to report incidents that do not disrupt or degrade services, making a higher reporting threshold problematic.

The results could favour government agencies over other vital service providers. Analysing only NIS-organizations can ignore attack frequency without consequence. Thus, “disruption bias” may affect cyber threat landscape interpretation. Results are based on incidents the reporting organisation considers reportable, which could cause disruption bias. Organisational reporting is autonomous. Second, incident taxonomies and data analysis are difficult. Content analysis was useful for studying IT incidents, but the researcher’s subjective categorization hampered the study. Researchers’ knowledge and interpretation of events determine research results. A structured incident classification could be beneficial, but this study struggled to create a report taxonomy. An abstract taxonomy is needed to classify IT-incident reports by characteristics, including indirect impact.

AVOIDIT and Cyber Harm use high-level classifiers to classify attacks, but the categories could be too abstract and fail to distinguish attack characteristics. The AVOIDIT taxonomy and categories may be outdated since 2009. More could have been done to represent relevant impact types. A weakness of this study is that it classified impact within and outside the cyberinfrastructure without measuring it. Although disruption and economic impact are primary informational and indirect impacts, the study does not account for total downtime or economic loss. Comparing cyberattack effectiveness is difficult.

6 CONCLUSION

The analysis of IT incident reports from Swedish service providers to MSB indicates that denial-of-service attacks and disruptions severely affect operations and information. Many of the 254 cyberattacks studied had no effect. Many social engineering attacks had little direct impact. Social engineering for initial access and user attacks is decreasing but still common. Infection with malware is rare. Few malicious IT incidents compromised critical service providers’ information resources. The indirect impacts were mostly economic. Supply chain incidents often impacted society and the economy. By identifying cyberinfrastructure’s impact types on service providers and others, this paper advances scientific understanding. This study found that many critical service provider cyberattack reports show no impact.

RQ1 suggests many cyberattacks have no social or organisational impact. This study supports previous findings on supply chain incidents and organisational and societal impact.Cyberattack classification and components could be studied. We lack incident taxonomies by high-level characteristics and affect. Methodological advances in cyberattack-classification that focus on possibilities and limits would benefit systematic analysis of cyber incidents based on reports with varying levels of detail. Research on incident severity using indirect impact indicators is needed. It categorised incidents by component. It would be important to study how DDoS attacks prolong critical service downtime.

REFERENCES

Agrafiotis, I., Nurse, J. R., 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), tyy006.

Applegate, S. D., & Stavrou, A. (2013). Towards a cyber conflict taxonomy. In 2013 5th International Conference on Cyber Conflict (CYCON 2013) (pp. 1-18). IEEE.

Calderaro, Andrea and Blumfelde, Stella (2022) Artificial intelligence and EU security: the false promise of digital sovereignty, European Security, 31:3, 415-434, DOI: 10.1080/09662839.2022.2101885

Braun, V., & Clarke, V. (2012). Thematic analysis. American Psychological Association.

Boin, A. (2019). The transboundary crisis: Why we are unprepared and the road ahead. Journal of Contingencies and Crisis Management, 27(1), 94-99.

Caldarulo, M., Welch, E. W., & Feeney, M. K. (2022). Determinants of cyber-incidents among small and medium US cities. Government Information Quarterly, 39(3)

Derbyshire, R., Green, B., Prince, D., Mauthe, A., & Hutchison, D. (2018). An analysis of cyber security attack taxonomies. IEEE European Symposium on Security and Privacy Workshops (EuroS&PW) (pp. 153-161). IEEE.

Harry, C., & Gallagher, N. (2018). Classifying cyber events. Journal of Information Warfare, 17(3), 17-31.

Hsieh, H. F., & Shannon, S. E. (2005). Three approaches to qualitative content analysis. Qualitative health research, 15(9), 1277-1288.

Lallie, H. S., Shepherd, L. A., Nurse, J. R., Erola, A., Epiphaniou, G., Maple, C.,& Bellekens, X. (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, 102248.

Markopoulou, D., & Papakonstantinou, V. (2021). The regulatory framework for the protection of critical infrastructures against cyberthreats: Identifying shortcomings and addressing future challenges: The case of the health sector in particular. Computer law & security review, 41, 105502.

Mancuso, V. F., Strang, A. J., Funke, G. J., & Finomore, V. S. (2014). Human factors of cyber attacks: a framework for human-centered research. In Proceedings of the human factors and ergonomics society annual meeting (Vol. 58, No. 1, pp. 437-441). Sage CA: Los Angeles, CA: SAGE Publications.

Osei-Kyei, R., Tam, V., Ma, M., & Mashiri, F. (2021). Critical review of the threats affecting the building of critical infrastructure resilience. International Journal of Disaster Risk Reduction, 60, 102316.

Panda, A., & Bower, A. (2020). Cyber security and the disaster resilience framework. International Journal of Disaster Resilience in the Built Environment, 11(4), 507-518.Ulrich, B. (1992). Risk society: towards a new modernity

Paté-Cornell, M-Elisabeth, and Marshall A. Kuypers. ”A Probabilistic Analysis of Cyber Risks.” IEEE Transactions on Engineering Management 70.1 (2021): 3-13.

Papakonstantinou, V. (2022). Cybersecurity as praxis and as a state: The EU law path towards acknowledgement of a new right to cybersecurity?. Computer Law & Security Review, 44, 105653.

Plachkinova, M., & Vo, A. (2023). A Taxonomy for Risk Assessment of Cyberattacks on Critical Infrastructure (TRACI). Communications of the Association for Information Systems

Pursiainen, C. (2018). Critical infrastructure resilience: A Nordic model in the making?. International journal of disaster risk reduction, 27, 632-641.

Rashid, S. Z. U., Haq, A., Hasan, S. T., Furhad, M. H., Ahmed, M., & Ullah, A. B. (2022). Faking smart industry: exploring cyber-threat landscape deploying cloud-based honeypot. Wireless Networks, 1-15.

Simmons, C., Ellis, C., Shiva, S., Dasgupta, D., & Wu, Q. (2009). AVOIDIT: A cyber attack taxonomy. University of Memphis, Technical Report CS-09-003.

immons et al., (2014) AVOIDIT: A Cyber Attack Taxonomy. In: 9th Annual Symposium on Information Assurance, pp. 12–22

Shevchenko, P. V., Jang, J., Malavasi, M., Peters, G. W., Sofronov, G., & Trück, S. (2023). The nature of losses from cyber-related events: risk categories and business sectors. Journal of Cybersecurity, 9(1).

Syafrizal, M., Selamat, S. R., & Zakaria, N. A. (2021). AVOIDITALS: Enhanced Cyber-attack Taxonomy in Securing Information Technology Infrastructure. International Journal of Computer Science & Network Security, 21(8), 1-12.

Whyte, C. (2021). European Union: Policy, cohesion, and supranational experiences with cybersecurity. In Routledge Companion to Global Cyber-Security Strategy (pp. 201-210). Routledge.

Høyland, S. A. (2018). Exploring and modeling the societal safety and societal security concepts–A systematic review, empirical study and key implications. Safety science, 110, 7-22.

Zouave, E., Bruce, M., Colde, K., Jaitner, M., Rodhe, I., & Gustafsson, T. (2020). Artificially intelligent cyberattacks. Swedish Defence Research Agency, FOI, Tech. Rep. FOI.