European Research Studies Journal
Volume XXVII, Issue 3, 2024

pp. 778-796

Cyberattacks as Threats in Supply Chains

Submitted 20/06/24, 1st revision 15/07/24, 2nd revision 16/08/24, accepted 30/09/24

Sylwia Konecka[1], Zbigniew Bentyn[2]

Abstract:

Purpose: *The purpose of this study is to investigate how cyber threats in supply chains are identified and assessed, with a particular focus on evaluating the utility of threat maps as tools for this purpose.*
Design/Methodology/Approach: *This research defines and classifies various types of cyberattacks, providing examples from real-world supply chain disruptions. A bibliometric analysis was conducted using the Web of Science (WoS) database, focusing on open-access materials from the past five years. The search included the terms "supply chain," "threats," "cyber," and "cyberattack." Additionally, secondary data from Statista were reviewed, and a pilot study utilising Check Point's ThreatMap was performed.*
Findings: *The study reveals that cyberattacks pose a significant threat to supply chains, but there is limited research in the fields of management and economics on this topic. The findings highlight gaps in understanding which countries and industries are most vulnerable, as well as the frequency of attack types. The analysis also uncovered discrepancies in the data from threat maps, suggesting these tools may not provide a comprehensive view of actual attack incidents.*
Practical Implications: *This research underscores the importance of developing real-time data tools for tracking cyber threats. It also suggests that healthcare and government sectors are particularly vulnerable to cyberattacks, and that future studies should examine the role of AI in enhancing supply chain security.*
Originality/Value: *The study identifies a gap in existing research on cyber threats in supply chains, particularly regarding the most affected industries and countries. It also provides insights into the limitations of threat maps and the need for interdisciplinary approaches, combining management, economics, and computer science, to ensure supply chain resilience.*

Keywords: *Supply chain, cyber threats, cyberattacks, vulnerability, threat maps, Industry 5.0, digitalisation, bibliometric analysis.*

JEL classification: M15, L20, O33.
Paper Type: *Research article.*

Acknowledgement: *This publication has been funded as part of the project 'Innovations and Modern Information Technologies in Supply Chain Management,' Poznań University of Economics and Business.*

[1]*Dr., Poznan University of Economics and Business, Institute of International Business and Economics, Poland, Sylwia.Konecka@ue.poznan.pl;*
[2]*Dr., Poznan University of Economics and Business, Institute of International Business and Economics, Poland, Zbigniew.Bentyn@ue.poznan.pl;*

1. Introduction

According to the World Economic Forum (WEF, 2024) report, cyberattacks rank as the fifth most frequently cited global risk by respondents (39%). This report, which is produced annually by the World Economic Forum in collaboration with Zurich Insurance Group and Marsh McLennan, is based on the opinions of over 1,400 global risk experts, policymakers, and business leaders. The findings for 2023 indicate negative short-term outlooks and deteriorating long-term outcomes.

Respondents were asked, among other things, to select up to the risks they believe are most likely to present a material crisis on a global scale in 2024. The top risk came from the environmental risk category – 66% of respondents identified extreme weather conditions. The second most cited risk was from the technological category – AI-generated misinformation and disinformation – at 53%. In third and fourth place were societal and/or political polarization (46%) and the cost of living crisis (42%), both classified under sociological risks (WEF, 2024).

Louis and Saleh (2024), who also examined the major risks to supply chains, indicated that cyberattacks, data breaches, and intellectual property theft can threaten the confidentiality, integrity, and availability of information, disrupting the smooth functioning of global supply chains. Such incidents can lead to financial losses, reputational damage, and operational disruptions (Louis and Saleh, 2024).

According to a literature review conducted by James Pérez-Morón (2021), researchers have focused on supply chain (SC) cyberattacks in recent years. Ariffin (2021) concentrated on cyberattacks facilitated by internet access, while Urquhart and McAuley (2018) examined the protection of industrial devices from online threats. Levy (2021) explored how cyberattacks increasingly target individuals or small organizations within the supply chains of larger entities.

Radanliev *et al.* (2020) identified a dynamic and self-adapting supply chain system supported by Artificial Intelligence and Machine Learning (AI/ML), enabling real-time intelligence for predictive cyber risk analytics. Etemadi *et al.* (2021) described the use of blockchain for robust cyber supply chain risk management (CSCRM) (Gourisetti *et al.,* 2019; Pournader *et al.,* 2019; Alazab, 2020; Dehghani *et al.,* 2020; Ram and Zhang, 2020; Etemadi *et al.,* 2021; Grima *et al.,* 2023; Auzina *et al.,* 2023).

The analysis of secondary statistical data also shows that cyberattacks have ranked among the top threats for at least five years. The relationship between these threats and disruptions in supply chains is evident.

This is illustrated in Table 1, which reveals that the two main threats are cyber incidents, consistently holding the second-largest threat position for five years, and business interruptions, including supply chain disruptions, which have consistently occupied the top position.

Table 1. *Leading Risks to Businesses in the U.S., 2018-2023 (in percentages)*

Leading risks	**Year**					
	2018	**2019**	**2020**	**2021**	**2022**	**2023**
Business interruption (incl. supply chain disruption)	39	40	37	46	50	45
Cyber incidents (e.g. cybercrime, malware/ransomware causing system downtime, data breaches, fines and penalties)	45	36	43	33	37	30
Macroeconomic developments (e.g. inflation, deflation, monetary policies, austerity programs)	–	–	–	–	–	30
Shortage of skilled workforce	11	14	16	11	25	27
Natural catastrophes (e.g. storm, flood, earthquake, wildfire, extreme weather events)	38	33	32	27	35	26
Fire/explosion	19	18	20	14	17	18
Energy crisis (e.g. supply shortage/outage, price fluctuations)	–	–	–	–	–	14
Climate change (e.g. physical, operational and financial risks as a result of global warming)	11	12	16	12	14	12
Changes in legislation and regulation (e.g. trade wars and tariffs, economic sanctions, protectionism, Euro-zone disintegration)	17	20	23	14	13	10
Market developments (e.g. intensified competition/new entrants, M&A, market stagnation, market fluctuation)	23	27	24	25	15	9

Source: *Allianz. (January 19, 2023). Leading Risks to Businesses in the United States from 2018 to 2023 (Graph). In Statista. Retrieved August 20, 2024, from https://www-1statista-1com-1s8fui2bx0028.han3.ue.poznan.pl/statistics/422203/leading-business-risks-usa/.*

In an earlier study, directors and risk managers in the U.S. reported in a 2022 survey that the most significant business risks were data loss, cyber extortion, and cyberattacks. These business risks, among others listed, incur increasing financial drawbacks that impact company spending and may necessitate insurance to mitigate potential risks. It is anticipated that by 2030, the directors and officers (D&O) liability insurance market in the U.S. will have grown to over 20 billion U.S. dollars.

NASCIO (2021) reports also indicate that cyber incidents, such as ransomware attacks and compromises to the software supply chain, pose a major threat, with 57% of CIOs identifying ransomware as their top cybersecurity concern. Other significant risks include natural catastrophes, skilled workforce shortages, and energy crises.

McKinsey & Company (2020) report that demand variability (32%), sole sourcing (28%), and long input lead times (27%) are key sources of supply chain vulnerability. In Latin America, major threats include corruption (40.2%),

government instability (23.6%), and economic shocks (16.9%), with cyberattacks ranked 8th at 1.4%. In Sub-Saharan Africa, poor infrastructure (35.9%) is the primary concern, with cyberattacks ranked 9th at 0.8%.

A supply chain attack, also known as a third-party attack, value chain attack, or backdoor attack, occurs when a hacker gains access to a business's network through third-party vendors or the supply chain. Supply chains can be vast and complex, making some attacks difficult to trace. Supply chain attacks often go unnoticed.

Over time, these attacks can cause significant damage and are harder to detect and prevent if suppliers do not adhere to stringent cybersecurity practices and use the best available tools. Cyber incidents can halt the operations of any business, affecting productivity, sales, order fulfillment, and customer satisfaction. In extreme cases, hackers can manipulate programmable logic controllers (PLCs) in manufacturing plants, negatively impacting brand quality and reputation, and even causing public safety issues (Mecalux, 2022).

These threats are increasingly concerning to companies. In 2021 alone, cybersecurity experts recorded a 15.1% increase in cyberattacks and data breaches compared to the previous year. This number is expected to continue rising due to dominant trends such as Industry 4.0 and the digitalization of processes that companies around the world are adopting. Industrial sectors and governments must respond to these trends by implementing solutions and strategies that enhance security and strengthen the entire supply chain (Mecalux, 2022).

Thus, the secondary statistical data indicates that cyberattacks represent a significant threat to supply chains, potentially affecting their vulnerability. Consequently, an investigation was undertaken to assess how this topic has been explored by researchers. A bibliometric analysis of the Web of Science (WoS) database was conducted for this purpose.

The analysis was carried out in the first half of August 2024. Keywords "supply chain" and "threats" were searched in All Fields, limited to publications from 2020 to 2024, and only materials available in Open Access were selected. The search yielded 477 results. To narrow this number, only materials that also contained the keyword "Cyber" were included, reducing the count to 57.

Further refinement of the keyword to "cyberattack" resulted in only 3 articles, none of which were from the fields of management or economics. Similarly, the initial search identified only 2 articles in the WoS category of Business, 2 in Economics, 2 in Operations Research Management Science, and one each in the categories of Green Sustainable Science Technology and Management. Cyberattacks appear to be of primary interest to researchers in the categories of Computer Science Information Systems (38% of articles) and Engineering Electrical Electronic (18%).

Another analysis was therefore conducted, this time for All Fields from 2020 to 2024 in Open Access, using the keyword "supply chain" and then searching for "threats" within these results. Only relevant categories were selected: Management (45 articles), Business (30 articles), Operations Research Management Science (30 articles), and Economics (15 articles). Of these 120 materials, only 7 addressed issues related to cybersecurity or cyber threats (Creazza *et al.*, 2022; Rymarczyk, 2020; Ocicka *et al.*, 2022; Pérez-Morón, 2021; Oral and Paker, 2023; Naz *et al.*, 2023; Akter, 2022).

The literature analysis in the Web of Science database suggests that, although the issue of cyber threats to supply chains is significant according to business experiences, it has not been extensively studied in the fields of management and economics. Essentially, these are all the source materials identified by James Pérez-Morón (2021). This represents a research gap, warranting further exploration.

Therefore, the subsequent part of this study aims to answer the following research questions: Which countries are most vulnerable to cyberattacks? What types of attacks occur most frequently? Which industries are most frequently affected by cyberattacks?

To address these questions, secondary data from the Statista database was analyzed, and a pilot study was conducted analyzing research results on cyberattacks from November 13 to December 14, 2023. The data was sourced from Check Point's ThreatMap service and includes information on the countries most vulnerable to cyberattacks, the most affected industries, and the types of malicious software most commonly used in these attacks.[3]

2. Cyber Risks in Supply Chains and Cyberattacks

While the existing literature generally includes several classifications for supply chain risks (Jüttner *et al.*, 2003; Manuj and Mentzer, 2008; Ho *et al.*, 2015), there are very few taxonomies specifically for classifying cyber risks within supply chains.

Faisal *et al.* (2007) presented a seminal paper identifying different information risks that can impact the supply chain. Gordon and Ford (2006) propose two categories of risks: Type 1 includes incidents of phishing and theft or manipulation of data or services; Type 2 covers cyberstalking and harassment, stock market manipulation, blackmail, and corporate espionage.

The National Cyber Security Centre, UK (2019) distinguishes cyberattacks into un-targeted and targeted attacks. Ghadge et al. (2020) propose a holistic classification of risk events that accounts for risks from external environments, internal activities,

[3]*The research was conducted by Z. Ciecierska for the thesis titled "Cyberattacks as a Threat to the Supply Chain" supervised by S. Konecka.*

and physical breakdowns, while Colicchia *et al.* (2019) emphasize the dimensions of confidentiality, privacy, and information integrity across different layers of the supply chain. Building on the existing literature on specific cyber and information risk items, a combination of various taxonomies could be adopted.

For example Colicchia *et al.* (2019) derived the following cyber risks: enterprise resource planning (ERP) system malfunction (Colicchia *et al.,* 2019), the crash of a company's website (Tran *et al.,* 2016), lack of network connectivity (Faisal *et al.,* 2007), malware (Deane *et al.,* 2009), data breaches (Boyson, 2014), damage to records (Zuo and Hu, 2009), and theft of credentials (Zuo and Hu, 2009). As previously mentioned, traditional literature on supply chain risk management has proposed several methods for "assessing" risks, primarily based on evaluating the dimensions of probability and impact on business (Hallikas *et al.,* 2004).

According to IBM, a cyberattack is defined as any deliberate attempt to steal, expose, alter, disable, or destroy data, applications, or other resources by gaining unauthorized access to a network, computer system, or digital device (IBM, 2024a). Cisco offers a similar definition, describing a cyberattack as "a malicious and intentional attempt by an entity to breach an individual's or organization's information system. Typically, the attacker benefits from this action" (Cisco, 2024).

In the literature, a cyberattack is characterized as "a disruption to the integrity or authenticity of data or information, also referred to as an attack on a computer network or cyberattack. Malicious code that alters program logic can result in errors in program output and data output errors. The hacking process involves scanning the Internet for systems with weak security controls and searching for poorly configured systems" (Uma and Padmavathi, 2013). Thus, a cyberattack can be viewed as a deliberate attempt to steal, alter, or destroy data, applications, or resources through unauthorized access by threat actors (Tyagi *et al.*, 2023; Noja *et al.*, 2021).

In the context of computers and computer networks, an attack is any scheme aimed at exposing, altering, disabling, destroying, stealing, or gaining unauthorized access. A cyberattack is a specific type of offensive maneuver targeting computer information systems, infrastructures, computer networks, or devices (Csrc.nist.gov, 2021). An attacker may be an individual or process attempting to access data, functions, or other restricted areas of the system without authorization, often with malicious intent. Cyberattacks are frequently part of broader contexts such as cyberwarfare or cyberterrorism.

Threat actors, defined as individuals or groups engaged in activities intended to cause harm in cyberspace, conduct attacks for various reasons, most commonly for financial gain. IBM identifies the following motivations: financial assets, financial data, customer lists, personally identifiable information (PII), other sensitive personal data, email addresses, login credentials, and intellectual property such as trade secrets or product designs (IBM, 2024a).

Their operational scope is broad, encompassing everything from minor thefts to acts of cyber warfare. Threat actors may employ methods such as malware, password theft, or eavesdropping.

IBM reports that "the average cost of a data breach is $4.35 million. This figure includes the costs of detecting and responding to the breach, downtime and revenue loss, as well as long-term damage to the company's reputation and brand" (IBM, 2023). The substantial financial and reputational costs associated with these activities underscore the necessity for organizations to implement effective preventive measures against cyberattacks.

Certain cyberattacks can be particularly costly. Ransomware attacks, for instance, can demand ransoms as high as $40 million. Criminal schemes involving the compromise of business email accounts (Business Email Compromise, BEC) can result in losses of up to $47 million in a single attack. Cyberattacks that compromise customers' PII can lead to loss of customer trust, regulatory fines, and potential legal actions.

Estimates suggest that cybercrime may cost the global economy $10.5 trillion annually by 2025 (IBM, 2023). This underscores the growing threat of cybersecurity and the increasing need for preventive measures. Consequently, investing in robust cybersecurity protection becomes imperative.

3. Classifications of Cyberattacks

Cybercriminals employ a wide range of sophisticated tools and techniques to execute cyberattacks on enterprise information systems, personal computers, and other targets. An INTERPOL impact assessment (Abnormal Security, 2020) related to cybercrime due to COVID-19 has shown a noticeable shift in focus, from independent personal computers or businesses to major corporations, government networks, and critical infrastructures.

Criminals are taking advantage of the rapid deployment of remote systems and networks to support staff working from home, leading to increased security vulnerabilities, which they exploit to steal data, generate profits, and cause disruption. Based on comprehensive analysis of data received from member countries and private partners, a list of cyber threats has been identified as "significant" in relation to the COVID-19 pandemic (Iakovakis *et al.,* 2021).

The classification of cyberattacks based on their operational impact is the most common and easiest to understand for individuals not directly involved in the cybersecurity industry. Therefore, this classification is prioritized in the discussion. The classification of cyberattacks based on operational impact includes the following actions:

- Misuse of Resources: Unauthorized use of IT resources. This definition can be expanded to include any IT-related function requiring certain privileges, which are abused (Kjaerland, 2005).
- User Compromise: Occurs when an unauthorized individual gains access to a user's account or data, often through various malicious activities.
- Root Compromise: Unauthorized acquisition of administrator privileges on a specific host, including elevated privileges beyond a regular user, such as administrative and/or root permissions on a particular system (Simmons *et al.*, 2014).
- Network Compromise: A website or web application exploiting security vulnerabilities to carry out an attack, often through techniques like cross-site scripting or SQL injection (Simmons *et al.*, 2014).
- Malware Installation: A cyberattack involving malicious software. There are various types of malware, such as cryptocurrency mining software, viruses, ransomware, worms, and spyware. The main goals include stealing information or identities, espionage, and service disruption (Pilarski, 2023).
- Virus: A form of installed malware defined as a piece of code that attaches itself to certain files and replicates automatically when the program is executed (Hansman nd Hunt, 2005).
- Spyware: A type of malware that discreetly collects information from the computer system without the owner's knowledge and consent.
- Trojan Horses: Disguised as useful programs or hidden in legitimate software to trick users into installing them. A remote access Trojan (RAT) creates a hidden backdoor on the infected device (IBM, 2024a).
- Worms: Self-replicating malicious programs that can spread between applications and devices without human interaction. Unlike viruses, which spread when a user runs an infected program, some worms can have more severe consequences. For instance, the WannaCry ransomware, which caused an estimated $4 billion in damages, was a worm that maximized its impact by automatically spreading across connected devices (IBM, 2024a).
- DDoS Attacks: Aimed at disrupting a server, website, or network by overwhelming it with traffic, usually from a botnet—a network of distributed systems controlled remotely by a cybercriminal using malware (IBM, 2024a). According to IBM, the global number of DDoS attacks increased during the COVID-19 pandemic. Attackers increasingly combine DDoS attacks with ransomware or threaten to conduct DDoS attacks unless a ransom is paid.
- Phishing Attacks: Email, text, or voice messages designed to trick users into downloading malware, sharing sensitive information, or sending funds to the wrong people. While most users are familiar with mass phishing scams—fake emails that appear to come from trusted brands asking recipients to reset passwords or re-enter credit card information—more sophisticated phishing scams, like spear phishing and business email compromise (BEC), target specific individuals or groups to steal valuable data or large sums of money. Phishing is just one form of social engineering—a class of tactics

and "human hacking" attacks that exploit psychological manipulation to entice or coerce people into taking unwise actions (IBM, 2024a).

This is one of many possible approaches. In the subsequent sections of the paper, which focus on the analysis of available statistical data on different types of attacks, additional cyber threats will be identified.

4. Examples of Cyberattacks on Supply Chains

In 2020, several cyberattacks were observed targeting key global supply chain players, including ransomware attacks on two major shipping lines, MSC Mediterranean Shipping Company S.A. and CMA CGM S.A., and the International Maritime Organization (Everstream Analytics, 2021). Additional notable incidents in 2021 involved SolarWinds Orion, Mimecast, Ledger, and Kaseya, as well as attacks on governments, COVID-19 vaccine researchers, and the healthcare supply chain. Examples of supply chain attacks are described by the UK's National Cyber Security Centre (2019). Here are some of them:

Third-Party Software Provider: Since 2011, the cyber-espionage group Dragonfly (also known as Energetic Bear or Havex) has targeted companies in Europe and North America, primarily in the energy sector. They compromised industrial control system (ICS) software by infecting legitimate files with malware, enabling remote access to affected systems. These attacks exploit the difficulty in detecting altered software at the source, relying heavily on the supplier's integrity (National Cyber Security Centre, 2019).

Website Builders: Cybercriminals often use supply chains to distribute malware widely. The Shylock banking Trojan, which targeted e-banking in the UK, Italy, and the USA, is an example. Attackers compromised legitimate websites via website builders, redirecting users to malicious domains where the malware was downloaded (National Cyber Security Centre, 2019).

Third-Party Data Stores: Many companies outsource data to third-party aggregators. In 2013, large data aggregators were compromised, allowing attackers to exfiltrate sensitive information through an encrypted channel. This breach impacted credit and supply chain management systems, exposing valuable business data (National Cyber Security Centre, 2019).

Watering Hole Attacks: These attacks target websites frequently visited by specific organizations. For instance, the VOHO campaign used such an approach to install remote access malware, granting attackers control over targeted systems (National Cyber Security Centre, 2019).

Examples in China include AISINO Credit Information Company and Microsoft Windows Hardware Compatibility Program. In June 2020, AISINO's tax software

was found to contain malware, affecting businesses in China. The exact method and objective remain unclear (ENISA, 2021). In 2021, attackers exploited Microsoft's code-signing process to distribute rootkit malware, primarily targeting the gaming industry in China (ENISA, 2021).

One of the most well-known examples of a cyberattack on a company and its supply chain is the case of Maersk. In June 2017, Maersk, a global shipping giant, was severely impacted by the NotPetya cyberattack, which initially spread as ransomware but quickly revealed itself as destructive malware. NotPetya exploited Windows vulnerabilities, locking computers and destroying data. Maersk, with its extensive global network and complex IT systems, was heavily affected.

According to Wired, Maersk reported a $200-300 million loss due to the attack, which disrupted critical systems and froze revenue from its container lines for weeks. The attack affected three of Maersk's nine business units (Greenberg, 2018). Despite the significant revenue loss and mitigation costs, Maersk maintained its profit expectations for 2017 and assured no data breaches occurred. However, their existing antivirus and patch management measures were insufficient against the attack (Greenberg, 2018).

Other companies also suffered due to NotPetya. FedEx briefly halted trading of its shares because of disruptions at its subsidiary TNT Express, and Merck reduced its earnings-per-share forecast by up to 36% due to disruptions in manufacturing and research. Reckitt Benckiser projected £100 million in revenue losses as it worked to restore its systems (Lord, 2020). The NotPetya attack underscored the vulnerabilities in global supply chains, causing delays and material shortages worldwide.

Companies dependent on Maersk had to seek alternative logistics solutions, driving up demand and prices for other carriers. This incident highlighted the fragility of modern supply chains and led to increased investment in risk management and cybersecurity. Governments and international bodies introduced stricter data protection regulations to bolster resilience against future attacks. The Maersk-NotPetya case demonstrates the critical importance of cybersecurity in global logistics and the need for robust risk management strategies to protect against such disruptions.

5. Countries most Frequently Affected by Cyberattacks

Data from Statista reveals significant variations in vulnerability to cyberattacks across countries and regions. In 2020, the Czech Republic was the most exposed country to cyberattacks in Central and Eastern Europe, followed by Estonia and Lithuania (NordVPN, 2020). Globally, the United States was the most targeted, with 65% of detected attacks between September and November 2022 aimed at U.S. organizations, a stark contrast to Japan's 8% and Brazil's 6%. During this period, Chile, India, and Peru saw fewer attacks, with Brazil being the primary target in

Latin America, accounting for nearly 56% of regional cyberattacks, followed by Mexico at 28% and Colombia at over 10% (Kaspersky Lab; Mundo en Línea, 2020).

As internet access grows in Latin America, the region has recorded the highest cyberattack rates globally in early 2020, with mobile browser attacks nearly three times the global average. This is exacerbated by a shortage of IT professionals. Notable recent attacks include those by the hacktivist group 'Anonymous Brazil' during the 2016 Rio Olympics and an increase in attacks on public institutions in Brazil in 2019. In response, Brazil introduced its first National Cybersecurity Strategy in February 2020.

In Europe, Germany had the highest rate of cyberattacks (58%) in 2023, followed by France at 53%. The UK and Belgium reported the lowest rates, at 48% and 46%, respectively (HISCOX, 2023). A 2023 survey indicated that 70% of global organizations were at risk of a material cyberattack within the next year, a 20% increase from the previous year. In the UK, 84% of Chief Information Security Officers (CISOs) perceived the country as having the highest risk, though this contrasts with other reports ranking the UK among the lowest for cyberattacks (Voice of the CISO, 2023; Proofpoint, 2023).

In late 2022, Lithuania, South Korea, and Italy reported the highest number of cyber threats per 100 scans (SurfShark, 2022). Following Russia's invasion of Ukraine in February 2022, Poland became a major target for cyberattacks, ranking sixth in Europe alongside Hungary, Cyprus, Slovakia, Estonia, and Belarus. Attacks on Polish public institutions rose from 1,214 per week in October 2022 to 2,316 per week, with the public utilities sector facing attacks at double the average rate (International Trade Administration U.S. Department of Commerce, 2023). Overall, countries with greater internet penetration, larger economies, and higher populations experience the most threats, as reflected in telemetry targeting BlackBerry clients worldwide (BlackBerry, 2022).

Surprisingly, our research using data from the website https://threatmap.checkpoint.com/ revealed that less developed countries are often the most frequent victims of cyberattacks. The countries experiencing the highest number of attacks included Mongolia, which appeared every day during the analyzed period, Nepal, which was also present daily, and Macau, which regularly featured in the rankings. Vietnam frequently ranked high, and the Philippines was often among the top. Other countries that frequently appeared at the top included Indonesia, Georgia, Kuwait, Ethiopia, Angola, Nigeria, and Taiwan.

Weekly data showed the following distribution: During the first week (November 13 - 19, 2023), the most attacked countries were Mongolia, Nepal, Macau, Vietnam, and Taiwan. In the second week (November 20 - 26, 2023), the list expanded to include Georgia, Kuwait, and the Philippines, and the healthcare industry began to appear more frequently as a target. In the third week (November 27 - December 3,

2023), Ethiopia and Angola emerged as prominent targets. By the fourth week (December 4 - 10, 2023), Mongolia, Nepal, and Macau continued to be top targets. In the final days of the study (December 11 - 14, 2023), Georgia and Nigeria joined the forefront of the list.

6. Industries Most Frequently Affected by Cyberattacks

Analysis of data available in industry reports indicates that the manufacturing industry is particularly vulnerable to cyberattacks, accounting for 25.7% of global cyberattacks in 2023 and nearly 60% of incidents among Operational Technology (OT) sectors in 2022 (IBM, 2024b). Finance and insurance follow closely, with 18.2% of global cyberattacks in 2023.

Among other OT industries, energy was targeted by 17% of the attacks, while water utilities saw about 1% of the global attacks for the year (IBM, 2023). Other vulnerable industries include professional services and retail. The healthcare sector is also highly susceptible, facing various types of attacks, with 63% involving network and application anomalies (Orange, 2022).

Also government organizations and critical infrastructure with 83% of respondents in a German survey considering them highly vulnerable (NTT, 2020). Government agencies have also seen a significant rise in cyberattacks, with incidents increasing from 40,000 to 100,000 between December 2022 and August 2023 (BlackBerry).

In 2023, the healthcare industry in the United States was again the most targeted by ransomware attacks. This industry also experienced the most data breaches as a consequence of cyberattacks. The critical manufacturing industry ranked second in the number of ransomware attacks, followed by government facilities.

Similar results were obtained from our own research. The industries most vulnerable to cyberattacks were education, government, and communication. These three industries were consistently listed each day, indicating their significant susceptibility to cyberattacks. Additionally, on certain days, the following industries were also notably affected: Healthcare, particularly on November 20, 21, 25, 26, and in December 2023; and Hardware on November 25, 2023.

In the first week of the study (November 13 - 19, 2023), the most affected industries were education, government, and communication. In the third week (November 27 - December 3, 2023), the most vulnerable industries were communication, education, and government, except on days when healthcare was predominant.

7. Frequency of Different Types of Cyberattacks

Based on industry reports, the following data on common cyberattack types were collected. For Windows systems in 2019, Trojans led malware attacks (64.31%),

followed by viruses (15.52%) (AV-TEST, 2020). Globally in 2022, multipurpose malware, including banking Trojans and botnets, accounted for 31% of attacks, with 35% in the Asia-Pacific region. Infostealers ranked second, particularly in APAC (15%) (Check Point, 2024). Emotet was the most frequently detected malware family in corporate networks. Major malware types from 2020-2021 included backdoors, downloaders, and worms (Orange, 2022).

In 2023, ransomware dominated global attacks, making up 70.13% of incidents and affecting 72.7% of businesses, up from 55.1% in 2018 (Sophos, 2024). IoT devices were the most targeted (33%), followed by mobile devices (28%) and corporate computers (27%) (Forrester Research, 2024).

In the U.S., phishing, smishing, and business email compromise were the leading causes of data breaches in 2023, with phishing responsible for over 50% of cybercrime in 2022 (Identity Theft Resource Center, 2024; Statista Technology Market Insights, 2023).

***Table 2**. Global malware types detected most frequently 2020-2021 (in percentages)*

Most commonly encountered types of malware attacks worldwide from October 2020 to September 2021	**(%)**
Backdoor	37
Downloader	17
Worm	16
C2	9
Spyware/Keylogger	6
Ransomware	6
Expoit Kit	3
Click fraud	3
Botnet Activity	1
Spam	1

***Source:** Orange (2022).*

From our analyses, the types of malicious software that ranked highest in cyberattacks were primarily phishing, which was the most frequently occurring type of attack, followed by mobile malware targeting mobile devices, adware in the form of advertising spyware, backdoor software enabling remote access to systems, botnet networks of infected computers, and cryptominer software used for cryptocurrency mining.

The most common types of malicious software were primarily Mobile, Phishing, and Adware. During the fourth week of the study (December 4 - 10, 2023), these same types of malicious software—Mobile, Phishing, and Adware—remained predominant. In the final days of the study (December 11 - 14, 2023), the predominant types of malicious software continued to be Mobile, Phishing, and Adware, consistent with previous periods.

8. Conclusions

Analysis of attack data based on surveys of opinions from high-level managers or board members does not provide conclusive results regarding which countries are most frequently affected by cyberattacks. The United Kingdom, for instance, has alternated between being ranked at the top and being among the countries less frequently impacted by attacks. Therefore, it can be inferred that it is best to use tools that provide real-time data on attacks and are offered by various entities.

Significant differences also emerged from the analysis of our own research. Literature suggests that highly developed countries with extensive use of modern IT tools are more frequently targeted.

However, our research indicates that countries with much less developed IT infrastructure were the ones being attacked. Of course, it must be considered that our study was preliminary and lasted just over a month. It has been shown that, due to the discrepancies observed, it would be beneficial to conduct the study over a longer period, such as an entire year. Seasonal patterns of attacks on identified countries might be a factor. Additionally, discrepancies could arise from the tools used for real-time attack identification, provided by different entities.

The most popular is the Norse map, which classifies the country of attack origin, attack type, target country, and displays a live feed of attacks. It also allows filtering of data by location and protocol. Check Point similarly shows attacking and target countries, along with a counter of the number of attacks that have occurred on a given day. FireEye presents data similar to the Norse and Check Point maps, additionally highlighting the top 5 targeted industries over the past 30 days.

The Digital Attack Map allows filtering of attacks by type and provides snapshots of notable attacks, as well as simplified graphs of the most active countries. Historical data extending back to June 2013 is also available. The Kaspersky map features a statistics section, provides an overview of data sources, and is highly interactive. Unfortunately, the question of which countries are most frequently attacked, in light of both secondary data and information from the map—our study utilized the Check Point map – remains unresolved.

The results regarding the industries most frequently affected by cyberattacks proved to be similar. Both secondary and our own research indicate that the healthcare and government sectors are the most commonly targeted. Secondary research also points to the manufacturing industry, while our own research highlights education and communication. In relation to the most common types of cyberattacks, the results of the secondary data analysis and our own research align.

Phishing and attacks on mobile devices were the most frequently reported in the past year. Spyware, backdoor, spam, and botnet were also indicated. In this area of

research, it is important to consider that the data may vary from year to year. As new technological solutions are introduced, new types of cybercriminals exploiting these tools almost immediately emerge.

It is worth noting that secondary research indicates that cyber preparedness varies not only by country but also by company size and sector, with some small and medium enterprises (SMEs) reporting lower levels of readiness. As of November 2023, only 32 percent of Italian SMEs reported being prepared to face a cyberattack and its consequences.

In comparison, around 20 percent of small and medium companies in Italy reported being ill-prepared, while nearly half of the surveyed enterprises indicated they were unprepared for the eventuality of a cyberattack (Generali, 2023). Thus, future research should also include an analysis of the size of companies affected by the attacks. Unfortunately, such data were not included on the website https://threatmap.checkpoint.com/.

It can be inferred that most attack maps are intended merely to illustrate what is happening, presenting only a very small percentage of actual attacks, as the data is carefully selected for visualization purposes. Therefore, one should not rely on their actual accuracy.

However, the fact remains that the average enterprise is targeted by a cyberattack every 1.5 seconds, making the threats very real, with as many as 93% of these attacks being phishing attacks carrying ransomware payloads. Thus, the maps provide a general insight into what is truly happening in the world of cybercrime.

They are insufficient for analyzing cyberattacks on supply chains. Therefore, a further area of research could be the analysis of AI tools that facilitate the maintenance of supply chain security, such as Splunk, IBM QRadar, Darktrace, Cortex XSOAR, Vectra AI. These tools and platforms assist organizations in monitoring, detecting, and responding to cyber threats, as well as in analyzing and securing supply chains against potential attacks.

Another concluding question might be whether the study of supply chains in the era of AI will become a domain of computer science, given that the capabilities of these tools for managing, for instance, cybersecurity within the supply chain may exceed the scope of knowledge from the field of management sciences.

Alternatively, has this already occurred, considering the results of the bibliometric analysis? In management sciences, the study of cybersecurity in supply chains may rely significantly on case study analyses. However, to ensure the responsiveness of supply chains, interdisciplinary actions are essential.

References:

Abnormal Security, 2020. Abnormal Attack Stories: WHO impersonation. (Online) Available at: https://abnormalsecurity.com/blog/abnormal-attack-stories-who-impersonation/.

Akter, S., Uddin, M.R., Sajib, S., Lee, W.J.T., Michael, K., and Hossain, M.A., 2022. Reconceptualizing Cybersecurity Awareness Capability in the Data-Driven Digital Economy. Annals of Operations Research.

Ariffin, K.A.Z. and Ahmad, F.H., 2021. Indicators for Maturity and Readiness for Digital Forensic Investigation in era of Industrial Revolution 4.0. Computers & Security, 105, p. 102237.

AV-TEST, 2020. Distribution of Leading Windows Malware Types in 2019 (Graph). In Statista. (Online) Available at: https://www-1statista-1com-1s8fui2sv001c.han3.ue.poznan.pl/statistics/221506/share-of-new-types-of-malware/.

Auzina, I., Volkova, T., Norena-Chavez, D., Kadłubek, M., Thalassinos, E. 2023. Cyber Incident Response Managerial Approaches for Enhancing Small–Medium-Size Enterprise's Cyber Maturity. In Digital Transformation, Strategic Resilience, Cyber Security and Risk Management (pp. 175-190). Emerald Publishing Limited.

Azab, M., Alhyari, S., Awajan, A., and Abdallah, A.B., 2021. Blockchain Technology in Supply Chain Management: an Empirical Study of the Factors Affecting User Adoption/acceptance. Cluster Computing, 24(1), pp. 83-101.

Blackberry, 2022. Global Threat Intelligence Report. (Online) Available at: https://www.blackberry.com/content/dam/bbcomv4/global/pdf/0408-Threat-ReportV17.pdf (Accessed 11 September 2024).

Check Point Software Technologies, 2024. Cyber Security Report 2024. (Online) Available at: https://pages.checkpoint.com/2024-cyber-security-report.

Cisco, 2024. (Online) Available at: https://www.cisco.com/c/en/us/products/security/common-cyberattacks.html?dtid=osscdc000283.

Creazza, A., Colicchia, C., Spiezia, S., and Dallari, F., 2022. Who cares? Supply Chain Managers' Perceptions Regarding Cyber Supply Chain Risk Management in the Digital Transformation Era. Supply Chain Management - An International Journal, 27(1).

Csrc.nist.gov, 2021. Cyberattack-Glossary | CSRC. (Online) Available at: https://csrc.nist.gov/glossary/term/Cyber_Attack (Accessed 11 September 2024).

CyberEdge, 2023. Annual Share of Organizations Affected by Ransomware Attacks Worldwide from 2018 to 2023 (Graph). In Statista. (Online) Available at: https://www-1statista-1com-1s8fui2bx0028.han3.ue.poznan.pl/statistics/204457/businesses-ransomware-attack-rate.

Dehghani, M., Mashatan, A., and Kennedy, R.W., 2020. Innovation Within Networks–Patent Strategies for Blockchain Technology. Journal of Business & Industrial Marketing.

Etemadi, N., Van Gelder, P., and Strozzi, F., 2021. An ISM Modeling of Barriers for Blockchain/Distributed Ledger Technology Adoption in Supply Chains Towards Cybersecurity. Sustainability, 13(9), p. 4672.

Forrester Research, 2024. (Online) Available at: https://www.verizon.com/business/resources/Tc61/reports/mobile-security-index-report.pdf.

Generali, 2023. Share of Small and Medium Enterprises (SME) in Italy that are Prepared to Effectively Face Cyberattacks as of November 2023 (Graph). In Statista. (Online)

Available at: https://www-1statista-1com-1s8fui2sv0026.han3.ue.poznan.pl/statistics/1453467/italy-sme-readiness-to-cyber-attacks/.

Gourisetti, S.N.G., Mylrea, M., and Patangia, H., 2019. Evaluation and Demonstration of Blockchain Applicability Framework. IEEE Transactions on Engineering Management, 67(4), pp. 1142-1156.

Greenberg, A., 2018. The Untold Story of NotPetya, the Most Devastating Cyberattack in History. Wired. (Online) Available at: https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.

Grima, S., Thalassinos, E., Cristea, M., Kadłubek, M., Maditinos, D., Peiseniece, L. (Eds.). 2023. Digital transformation, strategic resilience, cyber security and risk management. Emerald Publishing Limited.

Hansman, S. and Hunt, R., 2005. A Taxonomy of Network and Computer Attacks. Computer and Security.

HISCOX, 2023. Cyber Readiness Report 2022. (Online) Available at: https://www.hiscoxgroup.com/sites/group/files/documents/2022-05/22054%20-%20Hiscox%20Cyber%20Readiness%20Report%202022-EN_0.pdf.

Iakovakis, G., Xarhoulacos, C.-G., Giovas, K., and Gritzalis, D., 2021. Analysis and Classification of Mitigation Tools against Cyberattacks in COVID-19 Era. Hindawi Security and Communication Networks, Volume 2021, Article ID 3187205. (Online) Available at: https://doi.org/10.1155/2021/3187205 (Accessed 11 September 2024).

IBM, 2024a. (Online) Available at: https://www.ibm.com/us-en.

IBM, 2024b. Distribution of Cyberattacks across Worldwide Industries in 2023 (Graph). In Statista. (Online) Available at: https://www-1statista-1com-1s8fui2sv001c.han3.ue.poznan.pl/statistics/1315805/cyber-attacks-top-industries-worldwide/.

IBM, 2023. Operational Technology (OT) Industries Worldwide Most Frequently Targeted by Cyber Attacks in 2022 (Graph). In Statista. (Online) Available at: https://www-1statista-1com-1s8fui2bx0028.han3.ue.poznan.pl/statistics/1374010/cyber-attacks-ot-industries-worldwide/.

Identity Theft Resource Center, 2024. Annual Number of Cyber Attacks Resulting in Data Compromises in the United States from 2020 to 2023, by type (Graph). In Statista. (Online) Available at: https://www-1statista-1com-1s8fui2sv001c.han3.ue.poznan.pl/statistics/1367217/us-annual-number-of-cyber-attacks-leading-data-compromises-by-type/.

Interpol, 2020. Cybercrime: COVID-19 Analysis Report. Interpol, Lyon, France.

Kjaerland, M., 2005. A Taxonomy and Comparison of Computer Security Incidents from the Commercial and Government Sectors. Computers and Security, 25, pp. 522-538.

Louis, F. and Saleh, M., 2024. The Importance of Risk Management in a Globalized Supply Chain. ResearchGate. (Online) Available at: https://www.researchgate.net/publication/380316036_The_Importance_of_Risk_Management_in_a_Globalized_Supply_Chain.

Manuj, I. and Mentzer, J.T., 2008. Strategies for Managing Risk in Gobal Supply Chains. International Journal of Physical Distribution & Logistics Management, 38(3), pp. 192-223.

McKinsey & Company, 2020. Which Conditions Make Businesses Most Vulnerable to Value Chain Disruptions, Including COVID-19? (Graph). In Statista. (Online) Available at: https://www-1statista-1com-

1s8fui2bx0028.han3.ue.poznan.pl/statistics/1155422/conditions-supply-chain-vulnerability-gvc/.

NASCIO, 2021. Concerning the Continuity of Government, What is Your Top Cybersecurity Risk Today? (Graph). In Statista. (Online) Available at: https://www-1statista-1com-1s8fui2bx0028.han3.ue.poznan.pl/statistics/1287540/united-states-important-cybersecurity-risks-perceived-by-cios/.

National Cyber Security Centre, 2019. Supply Chain Security Guidance. (Online) Available at: https://www.ncsc.gov.uk/collection/supply-chain-security/supply-chain-attack-examples.

Naz, F., Kumar, A., Agrawal, R., Garza-Reyes, J.A., Majumdar, A. and Chokshi, H., 2023. Artificial Intelligence as an Enabler of Quick and Effective Production Repurposing: An Exploratory Review and Future Research Propositions. Production Planning & Control.

Noja, G.G., Cristea, M., Thalassinos, E., Kadłubek, M. 2021. Interlinkages between government resources management, environmental support, and good public governance. Advanced Insights from the European Union. Resources, 10(5), 41.

NordVPN, 2020. Cyber Risk Index. (Online) Available at: https://s1.nordcdn.com/nord/misc/0.13.0/vpn/brand/NordVPN-cyber-risk-index-2020.pdf.

Ocicka, B., Rogowski, W. and Turek, J., 2022. Industry 4.0 Technologies as Enablers of Sustainability Risk Management. Ekonomia i Prawo - Economics and Law, 21(4).

Oral, F. and Paker, S., 2023. Risk Assessment for Maritime Container Transportation Security. Journal of ETA Maritime Science, 11(4).

Orange, 2022. Security Navigator 2022. (Online) Available at: https://www.orangecyberdefense.com/global/white-papers/security-navigator-2022organizations-worldwide-by-type/.

Pérez-Morón, J., 2021. Eleven Years of Cyberattacks on Chinese Supply Chains in an Era of Cyber Warfare: A review and future research agenda. Journal of Asia Business Studies, 16(2), pp. 371-395. DOI: 10.1108/JABS-11-2020-0444.

Pilarski, G., 2023. Wojskowy Instytut Techniczny Uzbrojenia - Zeszyt 167 nr 5/2023, pp. 97-106. (Online) Available at: https://yadda.icm.edu.pl/baztech/element/bwmeta1.element.baztech-c21637f1-3ed3-444d-baa8-c93caf6ffd0d/c/Pilarski_167.pdf.

Pournader, M., Shi, Y., Seuring, S. and Kh, S., 2019. Blockchain Applications in Supply Chains, Transport and Logistics: a Systematic Review of the Literature. Special Issue: Blockchain in Transport and Logistics, pp. 2063-2081.

Proofpoint, 2023. (Online) Available at: https://www.proofpoint.com/us.

Radanliev, P., De Roure, D. and Page, K., 2020. Cyber Risk at the Edge: Current and Future Trends on Cyber Risk Analytics and Artificial Intelligence in the Industrial Internet of Things and Industry 4.0 Supply Chains. Cybersecurity, 3, p. 13.

Ram, J. and Zhang, Z., 2020. Belt and Road Initiative (BRI) Supply Chain Risks: Propositions and Model Development. The International Journal of Logistics Management, 31(4), pp. 777-799.

Rymarczyk, J., 2020. Technologies, Opportunities and Challenges of the Industrial Revolution 4.0: Theoretical Considerations. Entrepreneurial Business and Economics Review, 8(1).

Simmons, C., Ellis, C., Shiva, S., Dasgupta, D. and Wu, Q., 2014. AVOIDIT: A Cyber Attack Taxonomy. (Online) Available at:https://www.researchgate.net/profile/S-Shiva/publication/229020163_

AVOIDIT_A_Cyber_Attack_Taxonomy/links/544e58360cf2bca5ce90aebb/AVOIDIT-A-Cyber-Attack-Taxonomy.pdf.

Sophos, 2024. Shier, J. and Gunn, A. It's Oh So Quiet (?): The Sophos Active Adversary Report for 1H 2024. (Online) Available at: https://news.sophos.com /en-us/2024/04/03/active-adversary-report-1h-2024/.

Statista Technology Market Insights, 2023. (Online) Available at: https://www-1statista-1com-1s8fui2bx0028.han3.ue.poznan.pl/chart/30870/share-of-worldwide-cyber-attacks-by-type/.

SurfShark, 2022. (Online) Available at: https://www-1statista-1com-1s8fui2bx0003.han3.ue.poznan.pl/statistics/1351436/most-targeted-countries-cyber-threats/.

Tyagi, P., Grima, S., Sood, K., Balamurugan, B., Özen, E., Thalassinos, E.I. (Eds.). 2023. Smart analytics, artificial intelligence and sustainable performance management in a global digitalised economy. Emerald Publishing Limited.

U.S. Department of Commerce, 2023. Cyberattacks in Poland Occur Every 9 Minutes. Trade.gov. (Online) Available at: https://www.trade.gov/market-intelligence/poland-ict-cyberattacks-poland-take-place-every-9-minutes.

Uma, M. and Padmavathi, G., 2013. A Survey on Various Cyber Attacks and Their Classification. International Journal of Network Security, 15, pp. 390-396. (Online) Available at:https://pdfs.semanticscholar.org/ba7b/234738e80b02 7240e9bfd837bfba61c13e17.pdf.

Urquhart, L. and McAuley, D., 2018. Avoiding the Internet of Insecure Industrial Things. Computer Law & Security Review, 34(3), pp.450-466.