BIGS | Policy Paper

Brandenburg Institute for SOCIETY and SECURITY

Cyber Supply Chain Attacks

BIGS
BRANDENBURGISCHES INSTITUT für GESELLSCHAFT und SICHERHEIT

Esther Kern, Alexander Szanto

BIGS Policy Paper No. 10 / Juli 2022

This study was conducted within the framework of the EUREKA cluster ITEA3 for innovative, industry-driven and pre-competitive research and development projects in the field of software-intensive systems and services in the research project CyberFactory#1 (CF#1). The project was funded by the Federal Ministry of Education and Research (BMBF).

BIGS | Policy Paper

Brandenburg Institute for SOCIETY and SECURITY

Cyber Supply Chain Attacks

Esther Kern, Alexander Szanto

Report

edited by

Brandenburgisches Institut für Gesellschaft und Sicherheit gGmbH
Brandenburg Institute for Society and Security gGmbH

Executive Director
Dr. Tim H. Stuchtey

Dianastraße 46
14482 Potsdam

Telephone: +49-331-704406-0
Fax: +49-331-704406-19

E-Mail: direktor@bigs-potsdam.org
www.bigs-potsdam.org

TABLE OF CONTENT

LIST OF FIGURES AND TABLES

ABBREVIATIONS

C&C	Command-and-Control
CISA	Cybersecurity and Infrastructure Security Agency
CSCA	Cyber Supply Chain Attacks
ENISA	European Union Agency for Cybersecurity
MSPs	Managed Service Providers
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NSC	National Security Council
ODNI	Office of the Director of National Intelligence
PPD-41	Presidential Policy Directive 41 - United States Cyber Incident Coordination
RaaS	Ransomware-as-a-Service
SaaS	Software-as-a-Service
SEC	U.S. Securities and Exchange Commission
SMBs	Small to Medium-sized Businesses
UCG	Cyber Unified Coordination Group
VSA	Virtual System Administration

EXECUTIVE SUMMARY

Cyber operations targeting supply chains are not a new phenomenon. Cybercriminals, state actors, and state-backed hackers have long sought to infiltrate trusted third parties in supply chains. While the effort required to do so can be considerable, the benefits to malicious actors and the damage they can cause are immense, as all users, customers, and parts of a supply chain can become potential victims in one fell swoop. In this study, we examine attacks on cyber supply chains in more detail and attempt to provide a systemic insight into this area. Firstly, we classify different types of Cyber Supply Chain Attacks (CSCA). Secondly, two prominent case studies are outlined in detail to highlight the methods deployed by malicious actors, the potential damages, and the lessons learnt. Finally, we conduct an econometric analysis of listed companies that are part of supply chains and have been affected by a cyber incident. To gain an overall view of the economic and financial losses, we will include and compare both event studies and results from annual reports. The insights gained from this study are ultimately summarised in recommendations for action.

1 INTRODUCTION

A chain is just as strong as its weakest link. This is a common expression when it comes to the level of security of supply chains. Global value creation has become increasingly interconnected over the past years and decades and has now reached a turning point due to the COVID-19 pandemic and the Russian war of aggression in Ukraine. In view of these current crises and the resulting geostrategic consequences, it remains to be seen to what extent and by what means of cooperation and selection of strategic partners this kind of networking and interdependence of global supply chains will continue in the years to come.

Modern supply chains are digital, networked, data-driven and have countless interfaces. While on the one hand this enables demand-synchronised production, new business models to emerge and costs to be reduced, on the other hand dependencies on the individual elements of the supply chain have increased significantly and the entire network has become more opaque. This degree of interconnectedness increases with each supplier, product or application area. In this complex network, transparency is essential in order to identify possible vulnerabilities and dependencies at an early stage and to be able to take appropriate measures.

However, many companies do not have an overview of the numerous interfaces to their suppliers. As a result, complex supply chains are vulnerable to digital threats, as the risks to this wide-ranging and non-transparent network are often not recognised.

Against this background, we conducted an econometric analysis to determine the financial impact on affected companies that are part of a supply chain and whether there is a directly measurable correlation. Econometrics, as a branch of economics, aims to quantitatively determine among other things correlations that exist between eco-

nomic and non-economic variables in an economy within a certain period of time, for example to empirically test economic theoretical models.

Applied to our study, we measured the correlation of cyber incidents on companies that are part of a supply chain by examining merely publicly listed companies and thus considering the correlation between the publication of information of the cyber incident and the immediate reaction on the stock exchange.

Since these losses are initially accounting losses, at least until they are actually realised by selling shares at a lower value that can be attributed to the cyber incident, we additionally considered the losses reported in annual reports. By doing so, we intended to present the directly reported losses of the affected companies in a quantified way. However, some companies did not quantify damages in their annual reports or these information were not available at the time of our analysis.

To make these effects more tangible, we have decided to investigate two case studies in more detail by analysing five levels of observation. These include

- cyber breach characteristics,
- forensic analysis,
- subsequent (related) attacks,
- financial impact and
- lessons learned from the attack.

With this approach, on the one hand, we seek to quantify losses caused, for example, by collateral damage through interfaces in the supply chain. On the other hand, we want to take a closer look at supply chains, as it is a complex and very opaque network even for those involved.

However, our primary focus is on the economic implications, which we attempt to identify and whose concrete impact on business activities we intend to illustrate with the two case studies. By analysing the financial implications of cyber supply chain attacks (CSCA), we hope to raise awareness of the need for secure and transparent supply chains in business and contribute to companies identifying and closing unknown vulnerabilities. Companies need to take a closer look at their supply chain in order to manage their own cyber risks.

First, the study briefly describes the initial situation and makes a conceptual differentiation between targeted attacks and distributed attacks (Chapter 2). Next, the two case studies are presented for each type of cyber incident covering five levels of observation (Chapter 3). This is followed by the econometric analysis, which first introduces the methodological approach of event studies and the underlying data sources, before the results and the resulting findings are discussed (Chapter 4). Finally, the results of the analysis flow into recommendations for action (Chapter 5) before we warp up with the conclusion (Chapter 6).

2 SITUATION

In May 2022, the cybersecurity authorities of the Five Eyes (FVEY) nations (United Kingdom, Australia, Canada, New Zealand, and the United States) issued a joint alert, warning against the trend of cyberthreat actors targeting managed service providers (MSPs) to spread malicious cyberactivities. They provided guidance and best practices for MSPs and their customers to secure sensitive data.[1] The alert picks up on recent reports that saw an increase in such activities. MSPs are an attractive entry point into a supply chain. A report by N-able states that nearly all MSPs surveyed experienced an attack on their systems in the previous 18 months, and 90 per cent saw an increase in attacks since the start of the COVID-19 pandemic.[2]

At the same time, the National Institute of Standards and Technology (NIST) released its revised guidance on Cybersecurity Supply Chain Risk Management.[3] This is part of the NIST's response to the Executive Order 14028, Improving the Nation's Cybersecurity, which was released in 2021 by the Biden administration. The revision is also a response to the changing threat landscape and to the SolarWinds attack, which painfully disclosed the vulnerabilities of digital supply chains.

Malicious actors have been exploiting supply chains for some time, but Cyber Supply Chain Attacks (CSCA)[4] remain an underestimated problem, despite the fact that attacks exploiting vulnerabilities in supply chains have increased over time,[5] as demonstrated by the cases of SolarWinds and Kaseya. ENISA, the European Union Agency for Cybersecurity, estimates in its latest 2021 Threat Landscape report that there will be four times more cyber operations against supply chains in 2021 as compared to 2020.[6] This trend will continue to grow and become more sophisticated as international conflicts increase. Well-known groups such as Dragonfly have deliberately used suppliers to gain access to targeted companies since 2011, with these targets primarily in the energy sector. The group Orangeworm, whose activities were discovered by Symantec in 2018,[7] applies the same tactics by exploiting secondary targets in the manufacturing, information technology, or logistics sectors to gain access to the intended targets in healthcare. The FBI issued another warning at the beginning of 2020 about the group's activities and the tactical hacking of supply chain software vendors.[8]

Predictions that CSCA will become more common over the next decade are not surprising in the context of a global industry that will continue to be more and more connected. Industry 4.0 stands not only for more connection points within a factory, but also to the outside world as factory floors and machines become globally networked. Prior to the COVID-19 pandemic, Gartner, a market research and analysis company on developments in IT, published a survey on third-party risks. Gartner stated that 60 per cent of the surveyed organisations declared that they work together with more than one thousand suppliers, while 71 per cent mentioned that their supplier numbers had increased over the last three years.[9] A large number of third-party suppliers means it is becoming increasingly difficult for organisations to keep track of suppliers and potential vulnerabilities. Moreover, an increasing number of suppliers means that the risk of possible vulnerabilities leading to attacks is rising. While analogue supply chains have collapsed in the wake of the

1 See Cybersecurity and Infrastructure Security Agency (2022).
2 See N-able (2022).
3 See Boyens, J., Smith, A., Bartol, N., Winkler, K., Holbrook, A., & Fallon, M. (2022).
4 CSCA refers to cyberoperations directed against digital service providers and companies that develop software solutions on the one hand, and activities against companies that are part of a supply chain on the other hand.
5 See Identity Theft Resource Center (2021).
6 See European Union Agency for Cybersecurity (2021): p. 3.
7 See Symantec (2018).
8 See Thomas (2020).
9 See Byran (2019).

pandemic, many new digital nodes have been created. Many of these had to be set up rapidly under pressurised conditions, creating new potential vulnerabilities. A supply chain is only as strong as its weakest link. The importance of protecting and knowing one's supply chain will only increase in the coming years.

The following sections take a closer look at the economic costs and impact of cyberattacks on supply chains for companies. The first section provides a definition(s) of CSCAs. Even though these attacks are rising, there is a lack of consensus within the community on what constitutes a CSCA. For our purposes, we will examine them from two angles:

1. **Targeted attacks**, which in most cases are carried out by state actors or actors acting on behalf of the state

2. **Distributed attacks**, which in most cases are carried out by cybercriminals

We will later present the findings from our event study analysis of the economic impact of CSCAs. We will subsequently take a deeper look at two case studies:

1. The cyberattack on **SolarWinds** in 2020

2. The **Kaseya** hack in 2021

The former is an example of a targeted attack, while the latter is an example of a distributed attack.

2.1. Definition of Cyber Supply Chain Attacks

Before the findings are discussed in detail, this chapter provides an overview of CSCA definitions and clarifies the definition for the purposes of this study.

2.1.1. Targeted Attacks

One type of CSCA is an attack specifically targeted at end-to-end processes or designed to become operative by information- or operational technology connections. IT security company Symantec describes supply chain attacks as a kind of attack vector that exploits services and software of a third party to compromise the final target.[10] The concrete modi operandi differ in design and complexity, since CSCAs take many forms (for example, hijacking software updates or code injection into legitimate software). Consequently, there exists a spectrum of CSCAs from a taxonomic perspective. Reed et al. have worked towards a Cyber Supply Chain Framework and identified several key components of CSCAs.[11]

- **Carrier:** Firstly, CSCAs can target either one of several information technology components such as software, hardware, firmware, or system-related data and information.

- **Time:** Secondly, CSCAs have a timeframe that extends across the whole system acquisition cycle (pre-acquisition, acquisition, or sustainment).

- **Location:** Malicious activity can occur at any internal and external location within and between the supply chain, both physical and digital (for example, supply chain goods or data flow).

Nevertheless, according to a study by Symantec[12] and IT Security expert Leonid Belkind,[13] CTO of Symantec, there is one key component that describes CSCAs:

- **Intrusion via Trusted Third Parties:** This means that CSCAs do not attack the target dir-

10 See Symantec (2019).
11 See Reed et al. (2014).
12 See Ibid.
13 See Belkind (2019).

ectly, but indirectly via third parties that have access to the target network. Third parties can be external suppliers that are involved in the companies' operations. By using links and connections between the external supplier and the target company, the CSCA makes use of lower security measures between trusted parties.

- Another way of exploiting access by trusted third parties is through the intrusion of external IT software used by the target company. For instance, the attacker infiltrates software that is automatically updated by the target. In the case of the very harmful NotPetya attack in 2017,[14] it was the update of an injected accounting software that helped the attackers to infiltrate several target networks.

Therefore, the phenomenon of CSCAs has led to a shift in focus for cybersecurity analysts and practitioners alike. It is not sufficient to protect one's own network; additional measures must be taken to achieve endpoint security.

2.1.2. Distributed Attacks

While targeted attacks aim to infiltrate weak links in the chain to reach the actual target, there are also cyberattacks that exploit the infrastructure of supply chains to spread malicious software as widely as possible and thus make the attack surface as large as possible. Value chain- or third party-related breaches accounted for 80 per cent of corporate intrusions in the last 12 months, according to a mid-2020 survey conducted by OpinionMatters on behalf of BlueVoyant.[15] This is not surprising, considering that 77 per cent of the respondents stated that they have only limited visibility around their third-party vendors.[16] More than three quarters of the companies surveyed did not seem to have further insights into their suppliers' infrastructure, which is apparently often the cause and attack vector of malicious activities.

Although supply chain security has received more attention from the media and corporate management in recent years, some blind spots remain. A further neglected risk is that of collateral damage when one's own company is not the direct target of a cyberattack. This was highlighted by the NotPetya case, in which an attack on Ukraine's economy simultaneously affected global shipping, some major pharmaceutical and food production companies.

NotPetya demonstrated how deeply connected global networking is, but at the same time how vulnerable modern infrastructures are, even when not directly targeted. A centrally connected network has many advantages, especially from a potential savings perspective. However, it also provides the opportunity for a single (cyber-)attack to cripple an organisation and possibly affect all associated supply chains if they are not adequately protected.

Not only are software vulnerabilities important, but so are the organisation's objects of protection: assets and processes that maintain business continuity. Hence attacks that target production, distribution, or logistical operation along a supply chain can be equally considered a CSCA. In sum, a working definition for taxonomic purposes could be:

Cyber Supply Chain Attacks are threats that make use of trusted channels (external tiers, goods, and data) in the supply chain in order to compromise the final target, particularly via operational endpoint vulnerabilities. Furthermore, CSCAs in a broader sense are threats that directly impair operations at different points along the supply chain (for example production, distribution, and logistical operations from Original Equipment Provider (OEM) across Module or Supplier System (Tier 1) and Component Supplier (Tier 2) to Parts Supplier (Tier 3)).

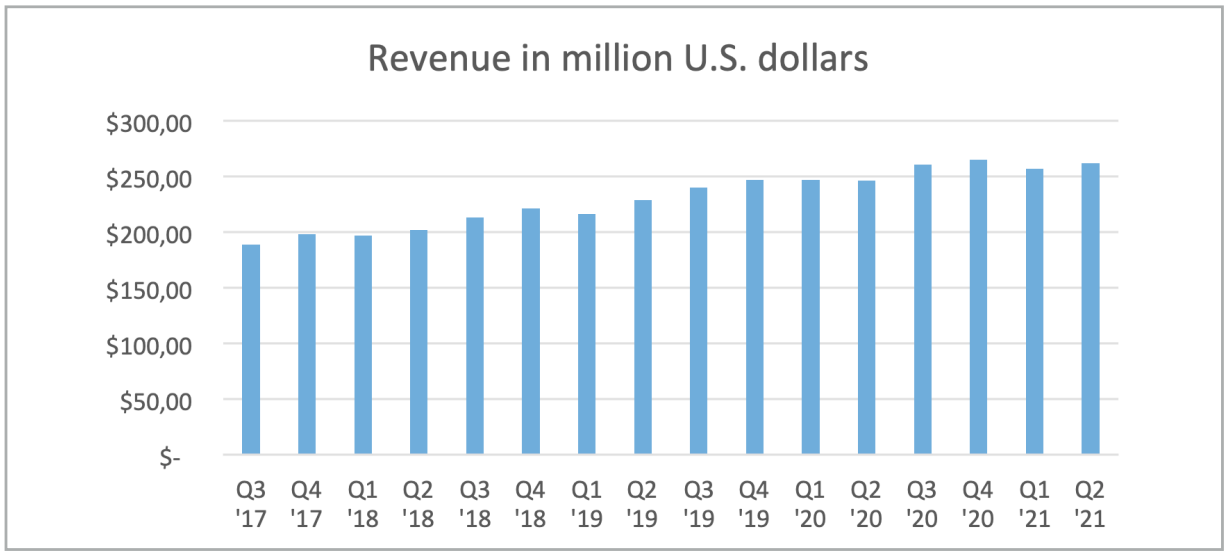
14 See Szanto (2019).
15 See BlueVoyant (2020).
16 See Ibid, p. 6.

3 CASE STUDIES

3.1. Case Study SolarWinds - USA

SolarWinds is a worldwide-operating IT management company headquartered in Austin, Texas, founded in 1999 by Donald Yonce and his brother David Yonce. The company focuses on network management software. SolarWinds aims at solutions that "give organizations worldwide, regardless of type, size or IT infrastructure complexity, the power to monitor and manage the performance of their IT environments, whether on-premises, in the cloud, or in hybrid deployments."[17] It was listed at the New York Stock Exchange from 2009 until the end of 2015, and again from fall 2018. Since 2007 it has experienced a large expansion of its product range due to numerous acquisitions in the areas of performance management, information security, network monitoring, database management, and data analysis. In 2011, Forbes ranked the company in as one of the fastest-growing tech companies.[18] One of its most known and most widely used software is the Orion platform, which is a scalable monitoring and management platform for the entire IT infrastructure. The company currently employs more than 2300 people worldwide and has over 300,000 customers in 190 countries, including in 498 of the Fortune 500 companies.[19] Well-known customers also include government entities worldwide.

Figure 1: SolarWinds Total Revenue from 2017 to 2021 by quarter in million U.S. dollars



Source: SolarWinds (2021c)

In July 2021, SolarWinds separated its managed service provider business into a separate company named N-able. SolarWinds as a company will focus on the IT management business, in particular IT infrastructure management software, while N-able will provide cloud-based software solutions for managed service providers.[20]

17 See SolarWinds (2021a).
18 See Harrell (2011).
19 See SolarWinds (2021b).
20 See Carlson (2021).

3.1.1. Cyber Breach Characteristics

On December 8th 2020, FireEye announced that it had been hacked and that some of its Red Team assessment tools had been accessed. FireEye is one of the most well-known cybersecurity companies worldwide. Their red tools are normally used to test the security of clients by mimicking the behaviour of cyberthreat actors. In this first statement, the CEO of FireEye, Kevin Mundia, declared that the "attack is different from the tens of thousands of incidents we have responded to throughout the years. The attackers tailored their world-class capabilities specifically to target and attack FireEye."[21] While this breach was already severe by itself, it is unlikely anybody expected this to be just the beginning of the discovery of the worst supply chain attack in the history of cyberattacks to date. Five days later, on December 13th, FireEye published their acquired knowledge about the attack.[22]

Later on the same day, the Cybersecurity and Infrastructure Security Agency (CISA) issued the Emergency Directive 21-01 *"Mitigate SolarWinds Orion Code Compromise"* to all government agencies, urging them to disable the versions of the SolarWinds Orion products that were compromised.[23] It was known at that time that at least one of the agencies of the Commerce Department was breached, and it was speculated upon whether the Department of Treasury was also affected (which was later confirmed).[24] That Sunday evening, SolarWinds finally confirmed the attack.

Figure 2: Screenshot of tweet by SolarWinds alerting their customers in Dec. 2020

Source: SolarWinds (2020a)

In a statement issued to news outlets by then-CEO Kevin Thompson, SolarWinds declared that:

"We are aware of a potential vulnerability which if present is currently believed to be related to updates which were released between March and June 2020 to our Orion monitoring products. We believe that this vulnerability is the result of a highly sophisticated, targeted and manual supply chain attack by a nation state. We are acting in close coordinate with FireEye, the Federal Bureau of Investigation, the intelligence community, and other law enforcement to investigate these matters. As such, we are limited as to what we can share at this time." [25]

On Monday December 14th, the company reported the case to the U.S. Securities and Exchange Commission (SEC).[26] In this context, the company also disclosed that it had notified around 33,000 Orion customers the day before, these being active customers during and after the period in question. SolarWinds added that it believed fewer than 18,000 customers had installed an Orion

21 See Mandia (2020).
22 See FireEye (2020).
23 See Cybersecurity and Infrastructure Security Agency (2020).
24 See Bing (2020).
25 See Panettieri (2020).
26 Since the Securities Exchange Act of 1934, public companies, certain insiders, and broker-dealers are required to make regular SEC filings. Regular reports are for example quarterly financial reports. The Form 8-K is used to disclose major developments to the company that might be of interest for investors. Cybersecurity incidents fall into this category and since 2011, the Commission has guidelines in place to assist companies with these filings. For more information, see United States Securities and Exchange Commission (2018).

product that contained the vulnerability. Already that Sunday, SolarWinds made a hotfix available to address the vulnerability at least partially and informed customers about additional mitigation step s.[27]

A first meeting of the National Security Council (NSC) was held on Saturday December 12th.[28] By Tuesday December 16th, the NSC announced the establishment of a Cyber Unified Coordination Group (UCG) on the basis of the Presidential Policy Directive-41 (PPD-41) framework.[29] PPD-41 is a presidential policy directive issued in July 2016 by the Obama administration on the coordination efforts and principles of the Federal Government's response to a cyber incident in the U.S. The UCG serves to coordinate between the different federal agencies in the case of a significant cyber incident and to integrate private actors if necessary.[30] The following week, a bipartisan group of U.S. senators demanded an investigative report by the FBI and CISA on the impact of the cyberattack on U.S. agencies,[31] opening the investigation through U.S. Congress.

Early on, cybersecurity experts as well as the U.S. government suspected a nation state was behind the attack due to its nature and sophistication. In early January 2021, the FBI, CISA, the Office of the Director of National Intelligence (ODNI), and the National Security Agency (NSA) issued a joint statement formally accusing Russia. More specifically, they stated that "this work indicates that an Advanced Persistent Threat (APT) actor, likely Russian in origin, is responsible for most or all of the recently discovered, ongoing cyber compromises of both government and non-governmental networks. At this time, we believe this was, and continues to be, an intelligence gathering effort."[32] In April 2021, the Biden administration imposed new sanctions against Russia in respond to the SolarWinds hack. In the Executive Order, the U.S. officially named the "Russian Foreign Intelligence Service (SVR), also known as APT 29, Cozy Bear, and The Dukes, as the perpetrator of the broad-scope cyber espionage campaign that exploited the SolarWinds Orion platform and other information technology infrastructures."[33]

It should not be overlooked that SolarWinds was only part of the puzzle. The attackers also used other initial infection vectors to compromise systems and approximately 30 per cent of the victims in both the private as well as the governmental sector had no direct connection to SolarWinds.[34] Furthermore, in February 2021, it became known that not only a Russian group, but also a suspected Chinese group, exploited SolarWinds software. While the attacks overlapped timewise, they are distinct and separate in nature.[35]

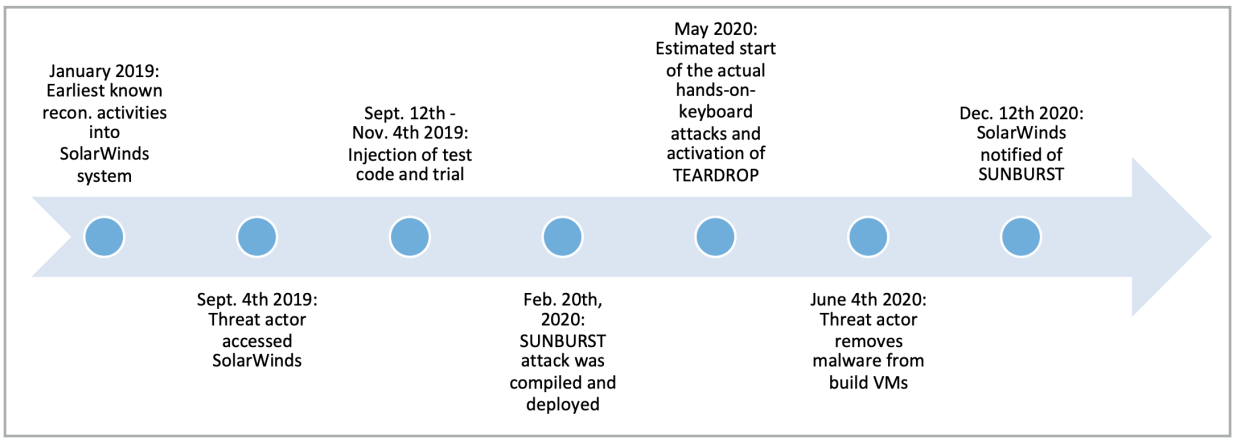
3.1.2. Forensic Analysis

"The attack unfortunately represents a broad and successful espionage-based assault on both the confidential information of the U.S. Government and the tech tools used by firms to protect them."[36] This is how the SolarWinds attack was described by Microsoft in December 2020. Further investigations into details and characteristics of the attack confirmed this assessment.

It later became known that the attackers were in the systems of SolarWinds as early on as January 2019. These first suspicious activities were of a reconnaissance nature. In September 2019, the attackers inserted a trial code, which did nothing other than to check which processor was running on a computer, and was thus more a proof of concept. The intruders wanted to examine "if it was possible to modify SolarWinds' signed-and-sealed software code, get it published and then later see it in a downloaded version."[37]

27 See United States Securities and Exchange Commission (2020).
28 See Bing (2020).
29 See Dunleavy (2020).
30 See The White House (2016).
31 See United States Senate (2020).
32 See Cybersecurity and Infrastructure Security Agency (2021).
33 See The White House (2021a).
34 See Kovacs (2021a).
35 See Bing/Stubbs/Satter/Menn (2021).
36 See Smith (2020).
37 See Temple-Raston (2021).

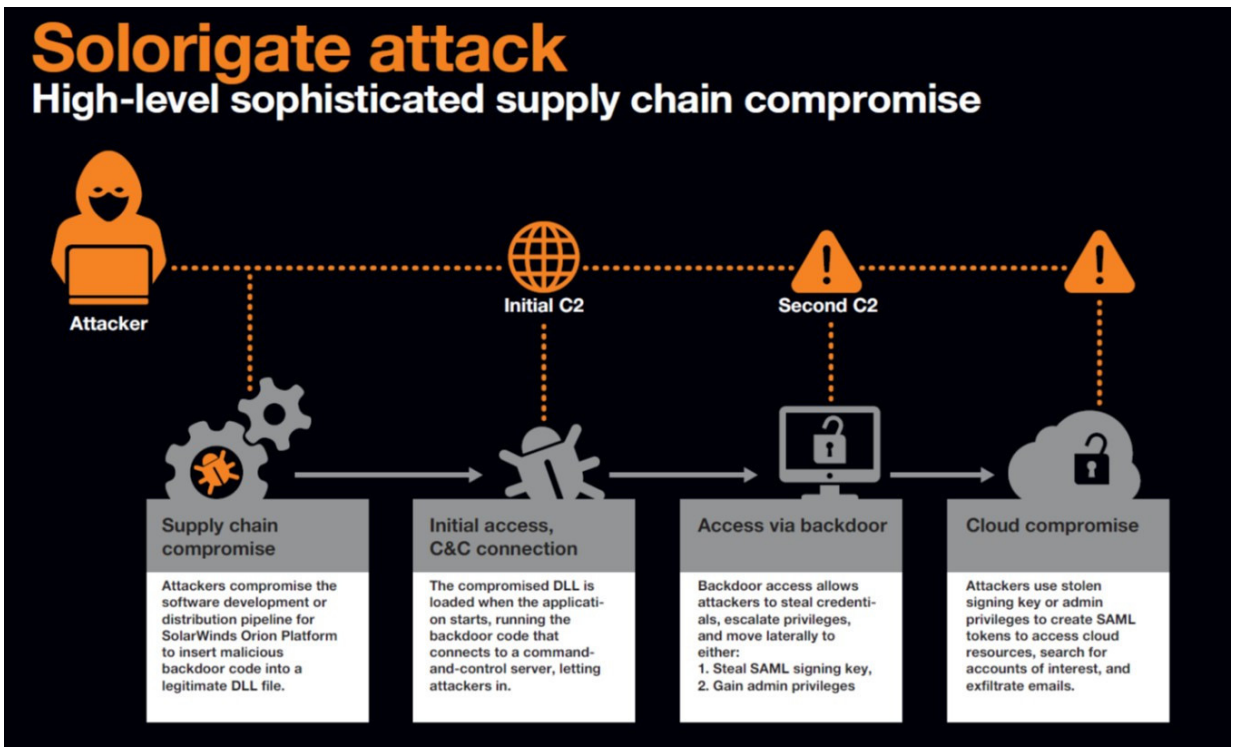
Figure 3: Timeline of SUNBURST Attack on SolarWinds Jan. 2019 – Dec. 2020



Source: Tucker (2021), Ramakrishna (2021a), Microsoft (2021)

The attackers made use of a routine update of the Orion software to install a first backdoor into the networks of possible victims. This backdoor was labelled SUNBURST. Since Orion is a network monitoring software, it must have access to all layers by default to monitor, analyse, and manage the overall network and IT infrastructure. Versions 2019.4 HF 5 to 2020.2.1 released between March 2020 and June 2020 were affected. For this initial entry, customers had to do two things: first, install and deploy the infected update of the Orion software, and second, have it on a computer that is connected to the internet.

Figure 4: SolarWinds supply chain compromise



Source: Orange (2021)

The attackers hid the malicious code in plain sight due to their ability to modify sealed software code. To avoid detection, they mimicked Orion's software communication protocols.[38] The malicious update was therefore properly digitally signed. Through this backdoor, the attackers had the possibility to communicate with the compromised infrastructure.[39]

An additional functionality of the backdoor is that it keeps a lookout for processes, services, and device drivers. Depending on what it finds, it alters its execution path and may abort execution. With the help of these checks, the code evaded detection, for example by anti-virus software. Overall, the attacker tried to behave inconspicuously.

When the SUNBURST backdoor is activated, it inspects the environment and gathers information. In doing so, it ensures that it is in the actual network and not on an analyst machine. It generally only becomes active after 12-14 days. Afterwards, it connects to a command-and-control (C&C) server through which it sends gathered information. This is the main execution stage. The backdoor can then be used to run commands by the attackers and send gathered information. Overall, the backdoor allows a wide range of commands, therefore allowing the attacker to "run, stop, and enumerate processes; read, write, and enumerate files and registry keys; collect and upload information about the device; and restart the device, wait, or exit." [40]

In some cases that the attackers deemed valuable or interesting, they activated a second-stage malware, using different loaders such as Teardrop and Raindrop for the Cobalt Strike Beacon.[41] "Cobalt Strike is a paid penetration testing product that allows an attacker to deploy an agent named 'Beacon' on the victim machine."[42] By doing so, a wide range of functions are available to the attacker, such as command execution, file transfer, or port scanning. Teardrop as well as Raindrop were used to load the Cobalt Strike Beacon; however, their configuration is different. The key difference is: "while Teardrop was delivered by the initial Sunburst backdoor […], Raindrop appears to have been used for spreading across the victim's network."[43] This post-compromise supply chain attack can then lead to attempts to elevate privileges, to steal credentials, or email theft.

Adam Meyers, the leader of the cyber forensic team that analysed the code for SolarWinds, described the hack as follows: "the tradecraft was phenomenal. […] The code was elegant and innovative. This was the craziest f***ing thing I'd ever seen".[44]

3.1.3. Subsequent (Related) Attacks

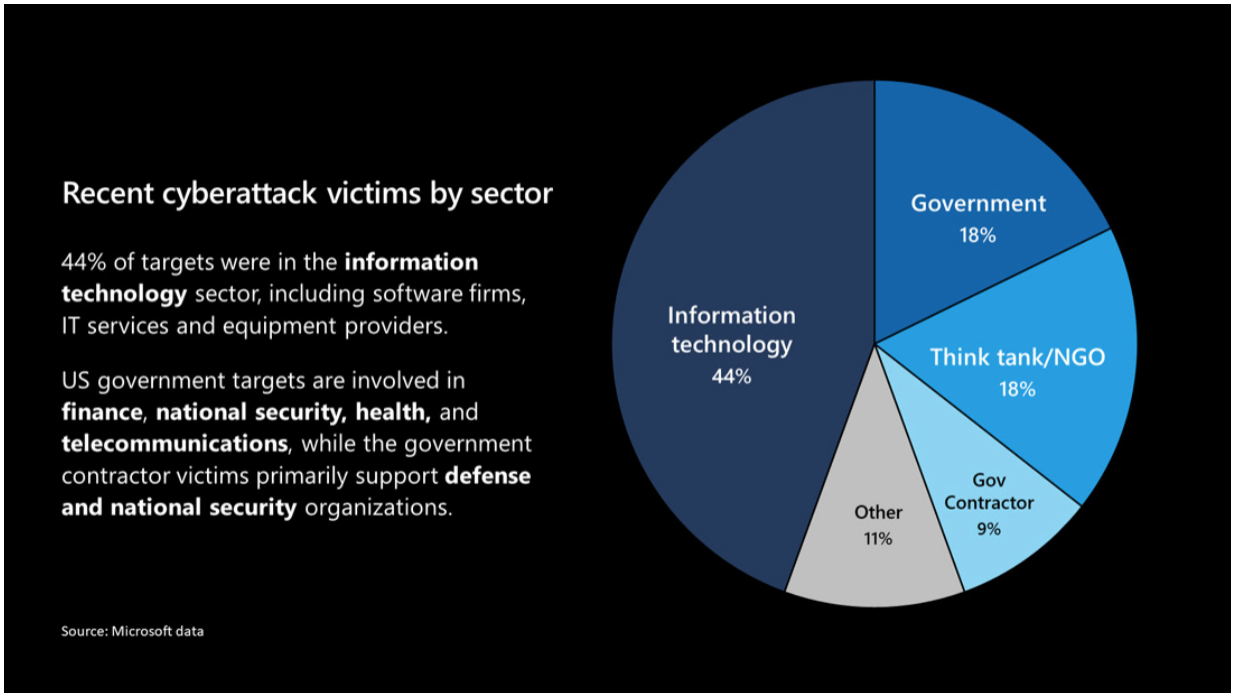
Over the course of the next weeks and months, more and more victims of the compromised Orion platform became publicly known. Among them were several U.S. agencies such as the U.S. Commerce and Treasury Departments, the Department of Homeland Security, and the National Institutes of Health and the State Department.[45] A joint statement by the Cyber Unified Coordination Group named fewer than ten U.S. agencies that were affected. Furthermore, while around 18,000 customers were exposed to the vulnerability, the number of organisations that experienced follow-up activities was much smaller.[46]

Microsoft declared in a statement that more than 40 of their customers were specifically targeted and compromised through further measures. While most of the companies were based in the United States, they identified victims in seven additional countries including Canada, the United Kingdom, and Israel. The majority of Microsoft's victims were from the information technology sector, including software firms or IT service providers. Microsoft itself detected malicious SolarWinds code in its systems, but stated that they

38 See Temple-Raston (2021).
39 See Viggiani (2020).
40 See Microsoft (2020).
41 See Microsoft (2021a).
42 See Fraunhofer-Institut für Kommunikation, Informationsverarbeitung und Ergonomie (2021).
43 See Symantec (2021).
44 See Temple-Raston (2021).
45 See Volz/McMillan (2020).
46 See Cybersecurity and Infrastructure Security Agency (2021).

did not find any evidence that the attackers had access to production services or customers' data, nor that their systems were used to attack others. They later reported that the attacker was able to examine small parts of Microsoft's source code.[47]

Figure 5: Recent cyber-attack victims that are customers of Microsoft by sector



Source: Smith (2020)

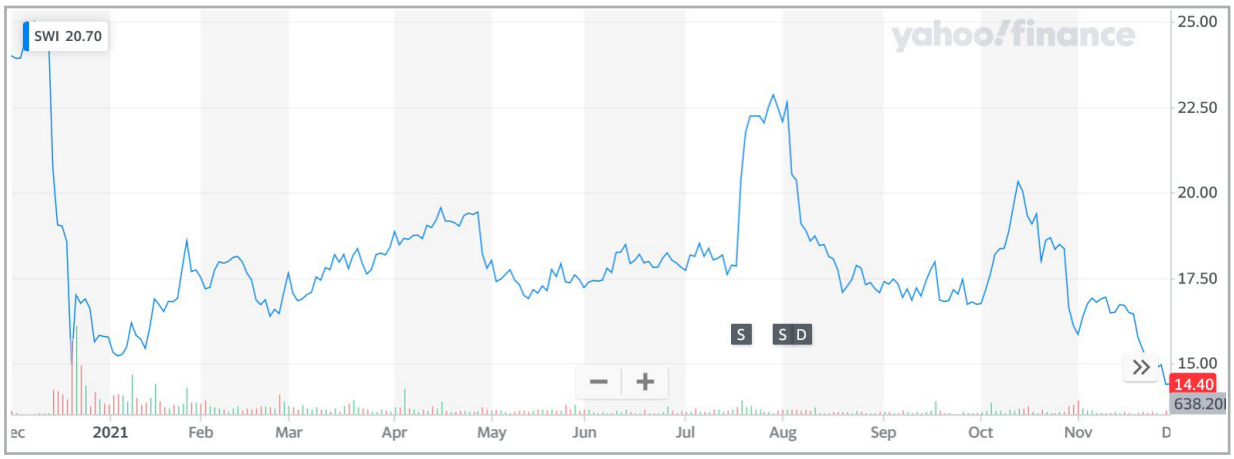
Among the victims were major information technology companies such as Cisco Systems and Intel. However, it is not clear in all cases whether the attackers actually took further steps once the malicious code infected the infrastructure of the respective organisations.[48] In other cases, such as the U.S. Treasury, email accounts were compromised and there was a breach involving the theft of encryption keys from U.S. government servers.[49] Cybersecurity experts state that while there were quite a few organisations that installed a backdoored SolarWinds Orion update, 99.5 per cent of these installations never progressed to Stage 2 operations, meaning the payload of one of the Cobalt Strike Beacons.[50]

47 See Microsoft (2021b).
48 See Poulsen/McMillan/Volz (2020).
49 See Tucker (2020).
50 See Hjelmvik (2021).

3.1.4. Financial Impact

The financial blow to the company was huge. On the first trading day on which the compromise became known to the wider public, the shares of the company dropped from nearly $25 to around $20, a loss of roughly 16 percent. The share price has not recovered since.

Figure 6: SolarWinds share price in the period December 2020 to November 2021

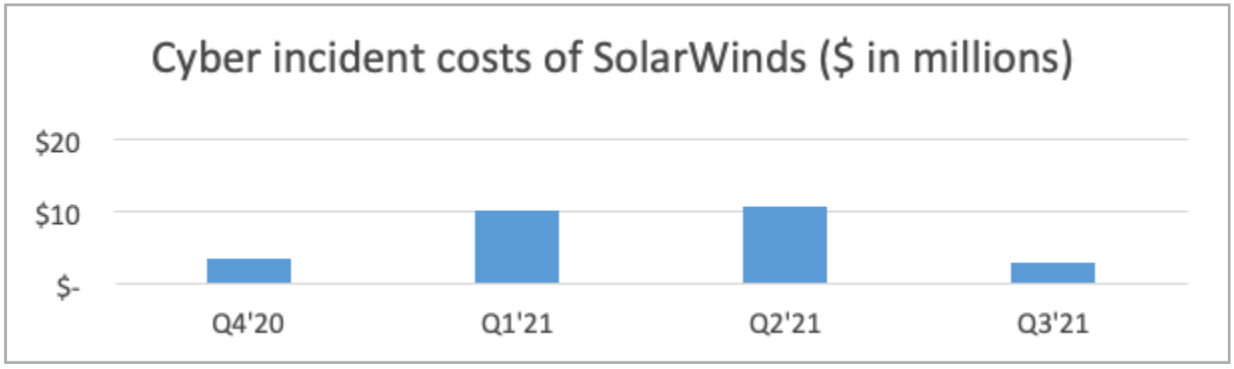


Source: Yahoo!Finance (2021)

Furthermore, in the course of December it became publicly known that two private equity companies – Thoma Bravo and Silver Lake Partners – had sold a significant amount of shares totalling around $280 million in stock just days ahead of the announcement of the breach. Rumours of insider trading circulated, although both firms stated that they were not aware of the breach on December 7th when the placement to sell was made.[51] The SEC announced that it would investigate the trades. The probe of the case is still ongoing.[52]

The company, however, not only suffered share losses, but also had to bear high costs in responding to the cyberattack. In its report for the fourth quarter of 2020, SolarWinds cited cyber incident costs of about $3.5 million.[53] These were just the costs for December 2020. Overall, the company stated costs of over $27 million in 2020 and 2021 (see *Figure 7*) Included in these costs are security initiatives, increases in insurance fees, and professional service fees.[54]

Figure 7: Cyber Incident Costs of SolarWinds 2020-2021



Source: SolarWinds (2021d)

51 See Harwell/MacMillian (2020).
52 See Johnson (2021).
53 See SolarWinds (2020b).
54 See Comeau (2021).

These are the costs for SolarWinds alone. An estimate by BitSight and Kovrr cites costs of about $90 million in insurance losses, which also includes costs for incident response and forensic services.[55]

3.1.5. Lessons Learned from the Attack

Kevin Thompson, the former CEO of SolarWinds, stated in an interview in October 2019 that "there was not a database or an IT deployment model out there to which his Austin, Texas-based company did not provide some level of monitoring or management."[56] This dominance became a problem and made it a valuable target for threat actors. One initial foothold was all that was needed to run all subsequent steps, creating a multiplier effect. The attack painfully pointed out how vulnerable cyber supply chains are.

The exploitation of a software that is essential and widely used by many organisations is a valuable target and gives an entry point for threat actors to other, often more secure, systems. It also shows the interconnectedness of IT systems and the ecosystem at hand. Organisations must consider not only the security of their own IT environment in risk analysis, but also their software supply chain. These attack vectors using software supply chains will become more common in the coming years and it will be impossible to fully secure the system. However, organisations can make it harder for attackers and build more resilient ecosystem. This is a task for the entire IT industry and their customers – be it the Fortune 500 companies, governmental organisations, or small to medium-sized businesses (SMBs). One response by the U.S. Government was to issue an Executive Order, "Improving the Nation's Cybersecurity", in May 2021. With this Executive Order, the Biden administration aims to address barriers to information sharing and establish cybersecurity requirements for government agency suppliers.[57]

Part of this task is that organisations should inquire about the software of their vendors and its security measures. It should also be clear that vendors conduct continuous security and risk assessments of their products, rather than just at one point in the lifetime of a software. However, it is also the responsibility of companies to ensure that the software they introduce into their networks does not make them vulnerable. After the attack, there were debates about the state of cybersecurity at SolarWinds and whether the company was devoting enough resources and effort to security.[58] There was in particular a debate after it became known that the password 'solarwinds123' was listed on GitHub until at least November 2019. SolarWinds stated that the password was for a third-party application and not to access their IT systems. Nevertheless, the question remains as to how the company processed security internally.[59] Sudhakar Ramakrishna, the CEO of SolarWinds, announced a shift to a truly 'security-by-design' approach by the company. He has published an 11-point plan, which names three primary areas SolarWinds aims to focus on, namely the internal environment, the product development environment, and the security as well as integrity of their products.[60]

The SolarWinds hack is another example of the importance of information sharing of cybersecurity events and the ability to connect the dots between different events that seem isolated, but are connected indeed. There were some early warning signs. Volexity, a cybersecurity company, had already noticed suspicious activity on a client's computer in July 2020, which they thought might be connected to an update by SolarWinds. However, they felt they did not have enough evidence to report it. In October 2020, Pablo Alto Networks discovered a backdoor, which seemed to be connected to the Orion platform. They worked with SolarWinds to determine the underlying cause but did not conclude that this was a supply chain attack.[61]

These revelations prove the need for a culture change in companies and the understanding that sharing relevant information can only help the whole industry. However, it also requires efficient

55 See Shah (2021).
56 See Satter/Bing/Menn (2020).
57 See The White House (2021b).
58 See Kovacs (2021b); see Temple-Raston (2021).
59 See Vaughan-Nichols (2021).
60 See Ramakrishna (2021b).
61 See Temple-Raston (2021).

information sharing within governments to ensure they can act in a coordinated way. This is a task for governments globally.

CSCAs rely on the fact that there are software interfaces and that suppliers have access to other networks, usually with certain privileges giving them the initial foothold needed. A zero trust mindset adopted by companies can therefore be an essential aspect of cyber defence. Zero trust assumes that a breach is possible rather than assuming that the inside network is essentially secure. This includes thinking about who has and who needs privileges within a network environment. Adopting a least privileged access strategy already makes organisations more secure against attacks by reducing the attack surface and minimising opportunities for lateral movement by intruders. Additionally, the zero trust mindset means a shift from assuming trust to explicitly verifying an access request.[62]

3.2. Case Study Kaseya - USA

Kaseya is an American software company founded in 2001. The company focuses on the development of software to manage networks, systems, and information technology infrastructure. Its main customers are managed service providers, which proved critical in the cyberattack. The company aims to manage, secure and automate IT, as stated on their website.[63] Kaseya describes itself as "the leading provider of IT and security management solutions for MSPs and […] SMBs."[64] Kaseya has a presence in ten countries with its headquarters in Miami, Florida and its international headquarters in Dublin, Ireland. Globally, over 40,000 organisations use at least one Kaseya software solution.[65] Due to the fact that Kaseya is not a publicly traded company, it is not required to publish its annual revenue. However, in an interview with CEO Fred Voccola, he stated that the company was valued at $2 billion in 2020, which increased to $3 billion in 2021. Voccola added that Kaseya saw revenue growth of about 20 percent to around $360 million. He announced that Kaseya has plans to become publicly listed by the end of 2021.[66] These plans seem to be delayed, most likely due to the ransomware attack in summer 2021.

3.2.1. Cyber Breach Characteristics

At midday on Friday July 2nd 2021, internal and external sources alerted Kaseya to a potential attack.[67] The vulnerability was detected in the Virtual System Administration (VSA) software. VSA is a remote monitoring and management software. Customers, mainly MSPs, can install VSA on their own servers (on-premises) or use a cloud offering hosted by Kaseya as a Software-as-a-Service (SaaS).

As a first quick and proactive measure, Kaseya shut down their SaaS servers and notified all their on-premises customers to also shut down their VSA servers to avoid being compromised. This may explain why only a small number of Kaseya's customers and their respective clients were affected by ransomware attacks or security breaches in their systems. All customers that experienced ransomware attacks were on-premises clients. Kaseya also notified the respective law enforcement agencies such as the FBI and CISA on that Friday. Furthermore, while activating their own incident response team, they also hired external experts to help them with the recovery.[68]

On the following Monday, July 5th, REvil, one of the most well-known cybercrime groups, publicly announced that they were responsible for the attack. For the exchange of $70 million in Bitcoin, REvil offered to publish a publicly available decryptor.

REvil is specialised in the blackmailing of companies. Furthermore, they offer Ransomware-as-a-Service (RaaS) for smaller groups that have less "manpower" and expertise. On their "reveal platform" on the Tor network, they publish the stolen data of blackmailed victims and also offer

62 See Weinert (2021).
63 See Kaseya (2021a).
64 See Kaseya (2021b).
65 See Osborne (2021).
66 See McHugh (2021).
67 See Kaseya (2021b).
68 See Kaseya (2021c).

Figure 8: Ransom note from REvil

Source: Schmidt (2021)

"negotiations", as in the case of Kaseya about a universal decryptor.[69] U.S. president Joe Biden had a call with Russian president Vladimir Putin in which he made it clear that he expects Russia to take action against groups such as REvil if they are operating on Russian soil (even if it was not a state-sponsored attack) in the case that the U.S. provides them with sufficient information about who was responsible for an attack.[70] Several days later, all of REvil's "dark" websites were suddenly offline. This included the payment and negotiation site. It is not clear whether the shutdown was initiated by Russian authorities following the phone call with Biden or whether the group shut down the websites itself. Another likely option is that Russia asked REvil to voluntarily shut down the websites while the group kept the entire ransom from various incidents.[71]

Kaseya gave its customers relatively quick access to a compromise detection tool to scan their systems for a potential breach. Customers that already had their systems encrypted were advised not to click on any links since these could be weaponised. Kaseya was able to fully bring back their SaaS infrastructure by July 12th and, at the same time, they made patches for on-premises customers available.

On July 22nd, Kaseya stated that they had obtained a universal decryptor key for victims of the REvil ransomware attack. It was stated that they had obtained it through a third party, though they did not clarify who that third party was.[72] They apparently did not pay for the key, or at least denied this publicly. Kaseya provided the decryptor key to some of the 1,500 victims of the ransomware attack.

In exchange for the key, Kaseya asked the respective organisations to sign a non-disclosure agreement. This was not confirmed by Kaseya spokespersons, but security experts working for some of the affected organisations confirmed this. However, this key came too late for most of the victims, since a majority had already painstakingly recovered their systems one by one through backups, or had chosen to pay the ransom.[73]

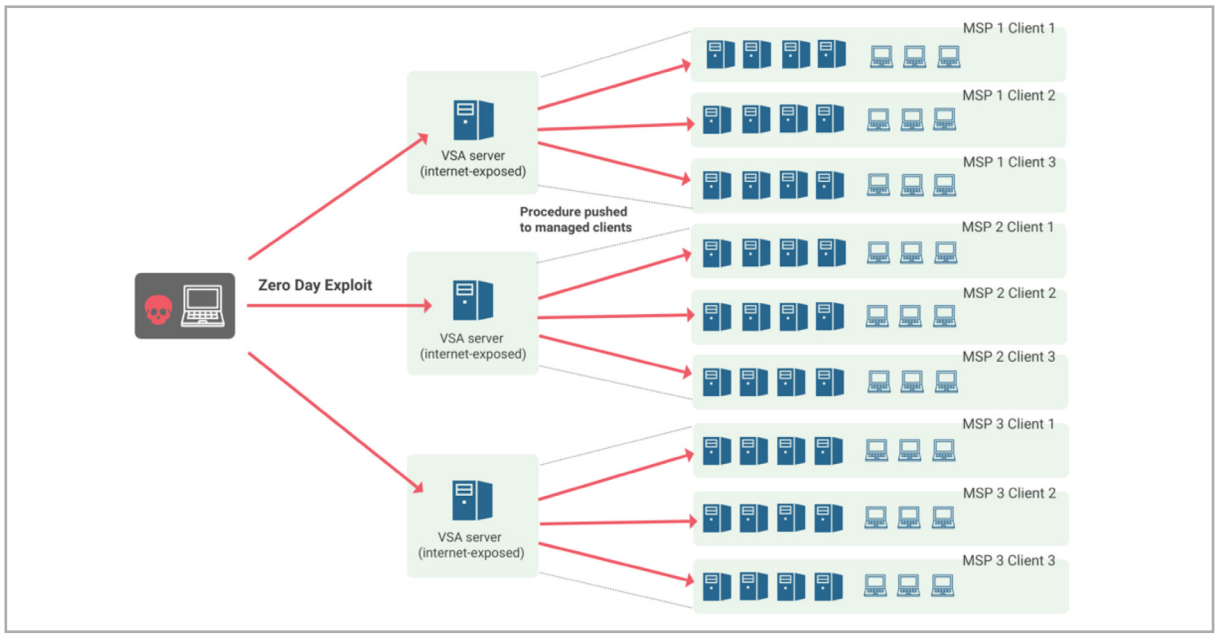
In November 2021, the U.S. Department of Justice announced an arrest of a Ukrainian national, charging him with conducting ransomware attacks, including the one against Kaseya. They also charged a Russian national with conducting Sodinokibi/REvil ransomware attacks against multiple victims while also seizing $6.1 million of alleged ransom payments.[74]

3.2.2. Forensic Analysis

REvil initially used a zero-day exploit to gain initial entry to the VSA server infrastructure. Afterwards, they had the ability to execute remote commands. This was used to send an alleged auto management update to VSA clients. Because MSPs normally have administrator rights into their customers networks, these updates also infected the clients of the MSPs.[75]

69 See Ibid.
70 See Finnegan/Nagle (2021).
71 See Greig (2021a).
72 See Kaseya (2021c).
73 See Greig (2021b).
74 See U.S. Department of Justice (2021).
75 See Beaumont (2021).

Figure 9: Overview of the Kaseya attack

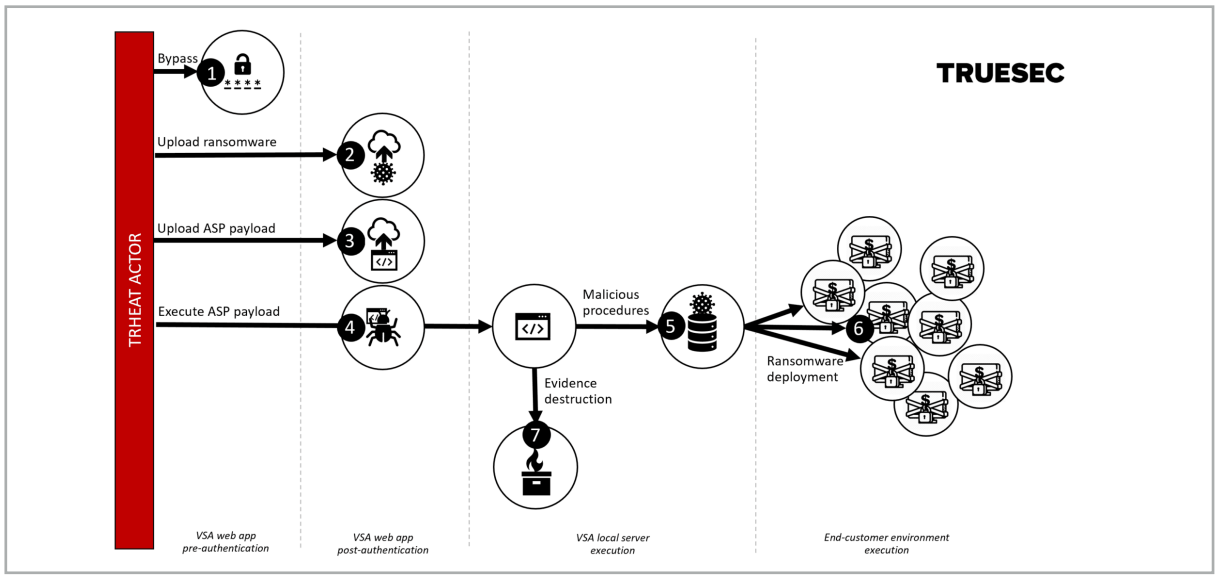


Source: Viggiani (2021)

Kaseya was made aware of this zero-day exploit through a coordinated disclosure and was preparing already a patch. Ultimately, however, they were not fast enough, as security researcher Victor Gevers states: "unfortunately, we were beaten by REvil in the final sprint, as they could exploit the vulnerabilities before customers could even patch."[76]

REvil used an authentication bypass for initial entry into the system in the Kaseya VSA web interface. This was possible due to a flaw in the authentication logic.[77] Therefore, they were able to "circumvent authentication controls, gain an authenticated session, upload a malicious payload, and execute commands via SQL injection, achieving code execution in the process." [78]

Figure 10: Attack Kill Chain of Kaseya attack

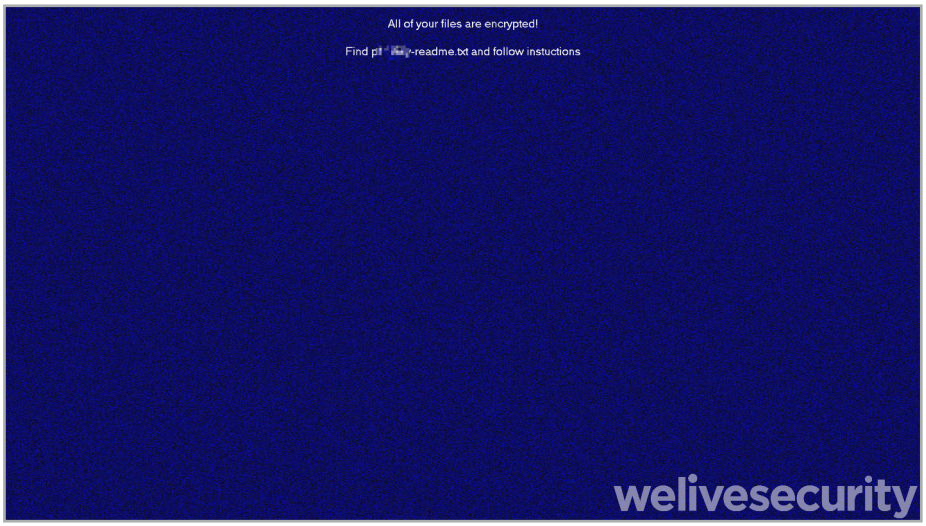


Source: Viggiani (2021)

76 See Gevers (2021).
77 See Andersson (2021).
78 See Osborne (2021).

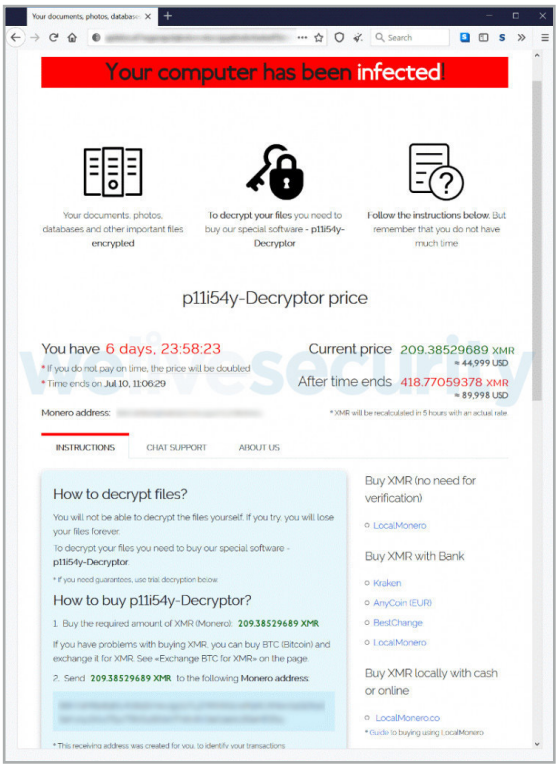
Once a server is infected, administrative access is shut down and the encryption process starts. When this process is complete, the desktop shows a blue image with the note that all files are encrypted, as seen in *Figure 11*. When a victim opens the link to the instructions, a readme text file opens. The link on the ransom note then leads to a page with the instructions for payment, as seen in *Figure 12*.[79]

Figure 11: System wallpaper after the completion of the encryption process



Source: Camp/Goretsky (2021)

Figure 12: Page with instructions on how to pay the ransom



Source: Camp/Goretsky (2021)

79 See Camp/Goretsky (2021).

3.2.3. Subsequent (Related) Attacks

MSPs (Kaseya's largest customer group) are responsible for managing the IT infrastructure of companies that outsource these services. Kaseya declared in a first statement that approximately 50 direct customers were impacted. However, more importantly, these MSPs are responsible for approximately 800,000 to 1,000,000 local and small businesses worldwide. In a first estimation, Kasey stated that 800 to 1,500 were compromised.[80] ESET Research declared that, based on their telemetry analysis, most of the reports came from the UK, South Africa, Canada, Germany, the United States, and Columbia.[81]

Figure 13: Victims of the REvil Ransomware Attack

Source: ESET Research (2021)

One of the most prominent victims was the Swedish supermarket brand Coop. Coop itself does not use the compromised Kaseya software. However, one of their IT service providers, Visma, does. Visma manages the payment systems for the supermarket. Due to the attack, the whole payment system of their cash register and self-service checkouts stopped working. Coop had to close around 500 stores and reboot the system.[82]

The Swedish pharmacy chain, Apotek Hjärtat, which runs over 390 pharmacies, was another victim that was also not a customer of Kaseya. They were also unable to take payments.[83] Overall, Kaseya states that less than 0.1 percent of their direct clients were compromised, but due to the nature of their customers, up to 1,500 companies globally experienced a ransomware attack.[84]

3.2.4. Financial Impact

Kaseya has not yet publicly stated how much the incident cost them. It can, however, be estimated from other known sophisticated cyberattacks that

80 See Kaseya (2021b).
81 See Camp/Goretsky (2021).
82 See Paganini (2021).
83 See Beaumont (2021).
84 See Osborne (2021).

the cost to Kaseya alone was several million U.S. dollars. The affected companies can be expected to face similar costs, either because they had to restore their systems, or because they paid for the ransomware.

3.2.5. Lessons Learned from the Attack

Timing is everything. The Kaseya attack was executed on the Friday before July 4th. This meant that, at least in the U.S., many people were already unavailable due to the holiday weekend. This is not the first time hackers have used windows of opportunity shortly before or during a holiday.[85] They know that this is the time when most organisations run low on staff, while defence mechanisms, as well as awareness, might not be as high as usual.

Furthermore, response time might be delayed under these conditions because key personnel are on vacation or cannot be reached. Delayed response time can lead to greater damages in the IT infrastructure of a company, which makes recovery more time-consuming, expensive, and possibly more difficult. Therefore, it is absolute critical for organisations to take this into consideration and ensure that their networks are not defenceless over holiday periods, and that key IT personnel can be reached in case of emergencies.[86]

Kaseya was communicating quite closely with its customers during the security breach and in particular during the downtime of the VSA SaaS. They regularly sent status updates, notified customers about next steps to take, and gave information on when services might be back or when patches could be expected for on-premises customers. However, attackers exploited this regular communication by sending phishing emails to customers. These were fake emails containing links and/or attachments that possibly contained malicious links. Kaseya responded by sending updates without links or attachments.[87]

Organisations must be aware that attackers might use certain opportunities to profit from security breaches. Organisations should therefore consider this possibility in incident response plans and prepare for the handling of such situations. This should include the communication aspect. Well-prepared crisis communication in response to cyber incidents is a benefit for organisations seeking to maintain their customers' trust.

Ransomware has been on the rise for years and the process has been professionalised. RaaS has also gained popularity. Nowadays it is possible to issue ransomware campaigns even without technical knowledge. This is also linked with international state behaviour in the realm of cyber norms and understandings of what constitutes responsible behaviour. In the case of Kaseya, the attack was coded to circumvent Russia by avoiding systems that have as their default language Russian or related languages from the former USSR region.[88] Russia is known for allowing cybercriminals to operate within their borders as long as they do not target Russian companies.[89] However, by allowing them to operate relatively freely, it endangers the integrity and security of the whole IT ecosystem.

Many organisations today rely on MSPs for their IT infrastructure. However, as the Kaseya attack shows, this can become a security risk. The vast majority of victims were not direct clients of Kaseya, but clients of the affected MSPs. MSPs already play a crucial role when it comes to cybersecurity, but with increasing digitisation and the rising complexity of the issue, their role will become even greater. It is therefore critical that companies consider MSPs as a potential attack vector in their risk assessment.

This includes considering the admin privileges MSPs have within their networks. Organisations should consider cybersecurity as a factor when choosing their MSP. On the other hand, MSPs must be aware that they themselves can pose a cybersecurity risk and can be used as an attack vector. This means they must consider their own cybersecurity standards and cyber hygiene. Consequently they can provide another cyber defence mechanism by preventing a supply chain attack already at the edge of their networks, rather than being the channel through which it spreads.

85 See Cybersecurity and Infrastructure Security Agency (2021b).
86 See Cybereason (2021).
87 See Kaseya (2021b).
88 See Mendrez/Kazymirskyi (2021).
89 See IronNet (2021).

4 FINANCIAL IMPACT

4.1. Stock Market Price Analysis and Evaluation

4.1.1. Methodology – Event Study

The ***Event Study Methodology*** is the main methodology used in analysing the effect of cyberattacks on the firm's value. This methodology became typical in finance following the pioneering work of Ball and Brown[90], Beaver[91] and Fama et al.[92] Commonly used in combination with signal theory, event study analysis is a branch of econometrics that attempts to measure the informational relevance of an event and analyses the reaction of stock prices following the release of new information. The primary focus is on quantifying the indirect costs caused by an unforeseen event, which have a long-time horizon and are more difficult to calculate than direct costs.[93]The premise of the method requires organisations under study to be publicly traded so that the market has the opportunity to adjust the capital value in response to a given event. Potential stock price changes are evaluated for the presence of **Abnormal Returns (AR)** over a given period.

According to this perspective, favourable (or unfavourable) information generates an increase (or decrease) in prices and therefore positive (or negative) abnormal returns. Moreover, the magnitude of variation is positive and highly correlated with the type of information revealed by the event. A key assumption of the event methodology is that the calculated ARs are not the outcome of a random event, but the outcome of the respective event analysed. However, the non-response of financial markets may arise from the lack of novel information captured by the event or from market inefficiencies.[94]

Three main concepts are applied in the event study methodology: **the estimation period, event window/observation period and the cumulative abnormal return (CAR).**

- The **estimation period** refers to the time window prior to the analysed event, upon which the researcher predicts the "normal" return corresponding to a chosen model. The length of the estimation period plays a crucial role in event studies, as it may affect the estimated model parameters and thus the significance of statistical tests.

- The **event window/observation period** refers to the time period encompassing the date of the event in which its effect on the market price is observed. Although the chosen time window varies in literature,[95] the trend is to shorten it to ensure that the measured effects are attributable to the event being analysed.

- The **Cumulative Abnormal Return (CAR)** is the difference between observed and theoretical profitability. The abnormal return is the key measure for event studies. The literature on models applied in event studies shows a tendency to favour a regression-based model, including a market model, whose performance is comparable to that of the **Capital Asset Pricing Model (CAPM)**. Moreover, the majority of studies address abnormal performance ranging from 0.5 percent to 1.5 percent, which is considered "realistic performance".

Applying the event study methodology, the impact of cyber attacks on firms that have experienced CSCAs and are listed on either NASDAQ or on national stock exchange markets is examined.

4.1.2. Data

In examining incidents, we considered security breaches in supply chains that affect individual organisations and are caused by targeted or distributed attacks or as collateral damage. As a first step, a database was created with various company information that is covered by the above definition. These include:

90 See Ball/Brown (1968).
91 See Beaver (1968).
92 See Fama/Fisher/Jensen/Roll (1969).
93 See Pirounias/Mermigas/Patsakis (2014).
94 See Dumontier/Martinez (2001).
95 See Peterson (1989).

Table 1: Categorisation of Cyber Supply Chain Attacks (CSCA) Cases.

Case (the synonyms used in the public for this kind of cyber attack)	**Company Name**	**Industry**
Number of Employees	**Revenue**	**Branches**
Country	**Continent**	**Date of Security Breach**
Date of Detection	**Date of Report**	**Kind of Publication** (own announcement of by third parties)
Attack Vector (for example malware, ransomware, phishing, brute force attacks, etc.)	**Exploited Vulnerability** (kind of technical, human, organisational exploitation)	**Point of Intrusion into Supply Chain**
Position in Supply Chain	**Infrastructure** (part of the critical infrastructure according to the Directive on Security of Network and Information Systems (NIS-Directive) of the European Union – ENISA or the Federal Office for Information Security – BSI)	**Attacker** (for example nation state actors, cyber-criminals, script kiddies, hacktivists, insider, etc.)
Motivation	**Modus Operandi**	**Damage** (with date; might change over time with new information disclosed)
Settlement (Lawsuits)	**Spending for Recovery of Business** (with date)	**Total Damage** (with date)
Amount in Mio. €	**Sources**	

Source: Own illustration

Following this classification and definition, cases from publicly available (open) sources were listed (34). From this, 13 companies (but 14 assets, as we distinguish between Maersk A – stocks with more voting rights – and Maersk B – stocks with fewer voting rights) were identified that were eligible for an event study based on the publicly available data. These companies were not deliberately selected (related to their market/business importance), nor are their event study characteristics specific to the company in question.

The **"event"** is defined as the date on which the circumstances of the incident or the incident itself was published, either by the company or by third parties such as the media, cybersecurity researchers, and so on. The **event day (t=0)** is to be distinguished from the date of the attack or intrusion, which might have occurred weeks, months, or even years ago. In an efficient market, a stock market reaction to the announcement of an event is usually expected immediately after a wider publication.

Moreover, the event day (t=0) also sets the date for the **event window/observation period** and the **estimation period** that is subsequently analysed. Against this background, we examined the methodological approach of relevant event studies that also focused on security breaches (see *Table 2*).

Table 2: Event Studies on Security Breaches.

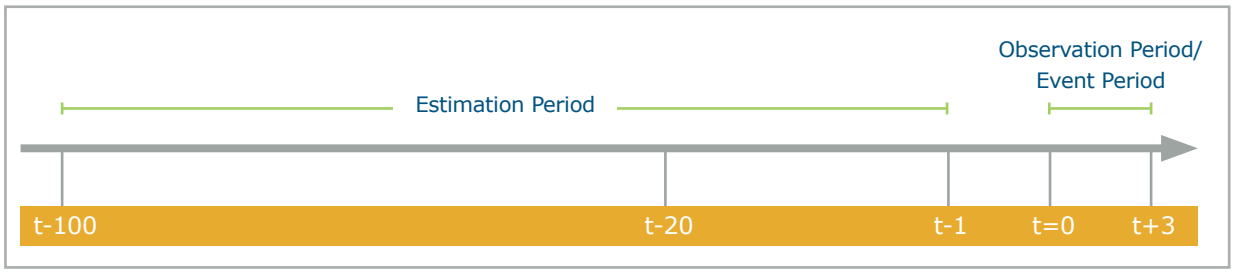
Author(s)	Type of Security Incident	Events	Time Frame	Method
Campbell et al. (2003)[96]	Security breach	43	1995 – 2000	Event Study (ES), 3-day Event Window (EW) [-1; 1], 120-day Estimation Period (EP) [-121; -2]
Cavusoglu et al. (2004)[97]	Security breach	66	1996 – 2001	ES, 2-day EW [0; 1], 160-day EP [-160; -1]
Kannan et al. (2007)[98]	Security breaches of any type	72	1997 – 2003	ES, 30-day EW [-1; 29], 50-day EP [-50; -1]
Gordon et al. (2011)[99]	All types of security breaches	121	1995 – 2007	ES, 3-day EW [-1; 1], 120-day EP [-121; -2]
Yayla and Hu (2011)[100]	All types of security breaches	123	1994 – 2006	ES, 11-day EW [-1, 1] [-1, 5] [-1; 10], 120-day EP [-130; -10]
Pirounias et al. (2014)[101]	All types of security breaches	105	2008 – 2011	ES, 3-day EW [-1; 1]; 200-day EP [-201; -2]

Source: Own illustration

Because increasing size of the event window/observation period also increases the risk of encountering other random events that may change the company's share price, a shorter event window/observation period is reasonable to reduce these effects. With the increasing length of the event window/observation period, the accuracy of the results obtained from an event study diminishes.[102]

In accordance with this theory and considering the analysed event studies (see *Table 2*), we chose an **event window/observation period of three days [0;3]** following the official publication of the security breach (see *Figure 14*). For daily event studies, the **estimation period** for evaluating normal returns typically varies between 100 and 300 days and ends one day prior to the selected event day (**t-1**).[103]

Figure 14. Selected Event Study Time Windows



Source: Own illustration

96 See Campbell/Gordon/Loeb/Zhou (2003).
97 See Cavusoglu/Mishra/Raghunathan (2004).
98 See Kannan/Rees/Sridhar (2007).
99 See Gordon/Loeb/Zhou (2011).
100 See Yayla/Hu (2011).
101 See Pirounias/Mermigas/Patsakis (2014).
102 See Fama (1991).
103 See Kritzman (1994).

The study sample includes data from the following assets: **Maersk A** (stocks with more voting rights), **Maersk B** (stocks with fewer voting rights), **Leoni AG, Norsk Hydro, X-FAB, Honda, Rheinmetall, Stadler Rail AG, UPS Logistics, Clarkson PLC, Mondelez Int., FedEx, Rockwell Automation,** and **Saint-Gobain**. Most companies published a press release on the incident, which served as the event day (t=0), whereas for Rockwell Automation we relied on newspaper releases.

Following the analysis of relevant event studies and the common methodological approach to determine the estimation period in daily event studies, we chose an estimation period of **100 trading days** prior to the event day (t-1).

Furthermore, we conducted a second analysis with a shorter estimation period of 20 trading days prior to the event day (t-1). This was motivated by the fact that some time series exhibited a high degree of noise over the entire period, as can be observed in Figure 15 (100 days). The approach of relying on daily stock returns is consistent with Morse[104] and Brown and Warner.[105] The estimation period of 100 trading days is intermediated to Brown and Warner, who collected data for 250 days, and Sinanaj and Zafar,[106] who applied 44 daily returns prior to the incident for their study of data breaches and stock returns.

Following Beaver,[107] we collected the closing price for each trading day, which is the final price of each daily trading session. The decision to utilise closing prices was taken for availability concerns, but not because it is the only suitable and appropriate variable. Closing prices only display the last price of the trading day and therefore provide only limited information on price trends. An alternative would be to take the daily average share price, as this can present a more precise picture of the overall price development. A further concern was related to our sample containing stocks from differently organised stock exchanges that differed in their public order book policies. We therefore reached the pragmatic decision to collect closing prices as raw data. In calculating returns, we followed the most commonly used **Mean-Adjusted Return (MAR)** formula as described, for example, by Brown and Warner:[108]

$$A_{i,t} = R_{i,t} - \bar{R}_i,$$

…where $R_{i,t}$ designates the observed daily return for stock i at day t. $\bar{R}_i$ describes the average daily return of stock i for the observed period. A_(i,t) covers the abnormal return for stock i at day t; this variable can be interpreted as the extent to which realised returns on the event day deviate from the returns that would be expected. Thus, as Campbell et al.[109] noted, abnormal returns can be considered a prediction error.

To assess the impact of a cyber incident on stock market returns for suppliers, we proposed the customary null hypothesis.[110]

Null hypothesis H0: There is no stock market reaction after information on a cyber incident has been released.

In testing our H0, we used a simple two-sample t-Test with equal variances on the mean of abnormal return before and after the event. In statistics, t-Tests are a type of hypothesis test applied to compare means. Since they reduce the sample data to a number, the t-value, they are called t-Tests. This tests for statistical differences in the mean of abnormal returns in the post-event period versus the pre-event period. Figuratively speaking, it tests whether any jumps at time t are significant.

4.1.3 Results

Figure 15 (100 days) shows the respective **Cumulative Abnormal Returns (CAR)** for the 100-day estimation period, and *Figure 16* (20 days) displays the CARs for the 20-day estimation period in our

104 See Morse (1984).
105 See Brown/Warner (1985).
106 See Sinanaj/Zafar (2016).
107 See Beaver (1968).
108 See Brown/Warner (1985): p. 6.
109 See Campbell et al. (2003): p. 441.
110 See Ibid: p. 435.

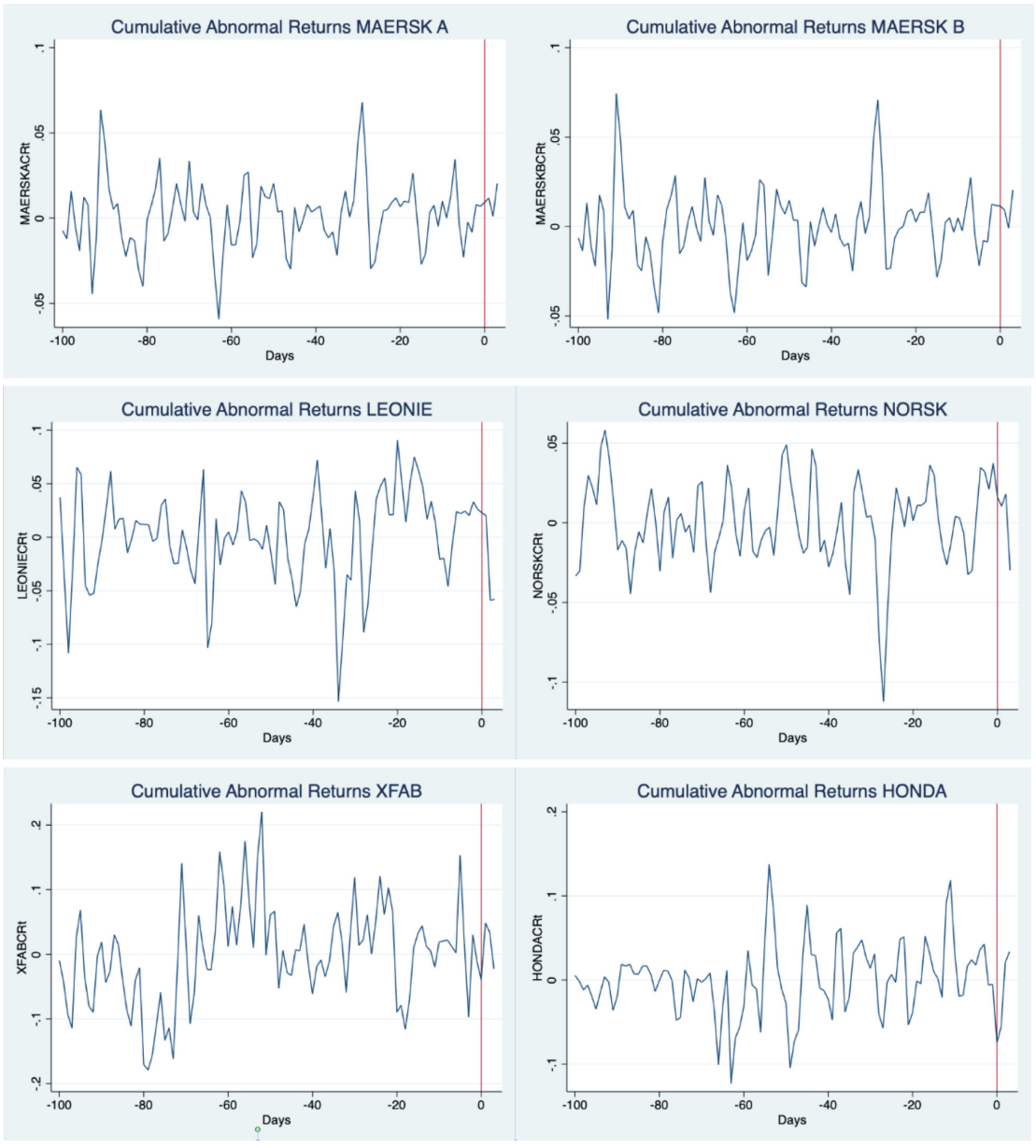
sample. *Table 3* contrasts the results (by company) in a two-sample t-Test and displays the comparison to actual losses reported in the annual report.

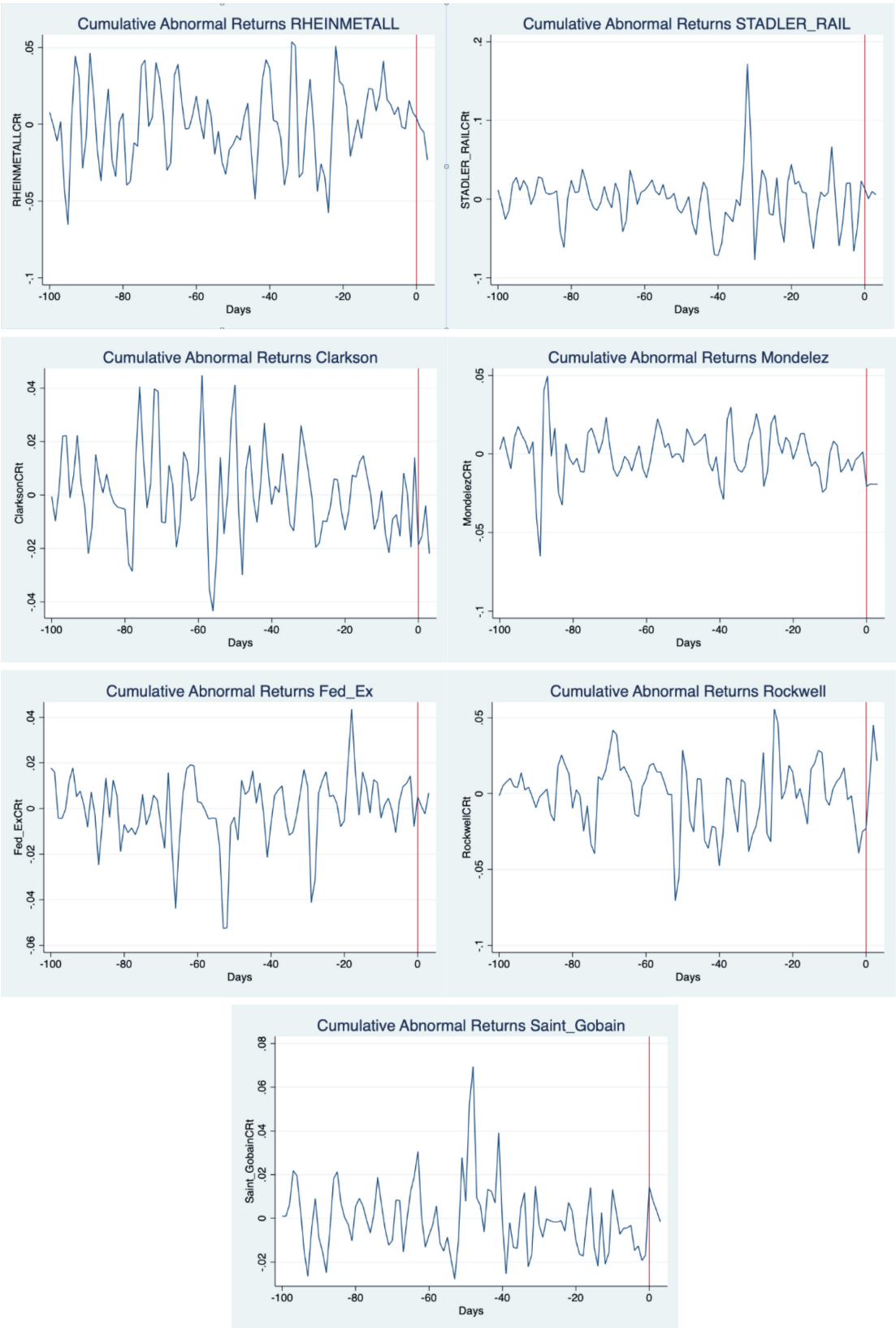
The **CAR** over the event window [t=0; t=3] is calculated as follows:

$$CAR_i = \sum_{t=0}^{t=3} AR_{i,t}.$$

Figure 15 (100 days) and F*igure 16* (20 days) show the CAR on the y-axis for the stock market performance of each company. Consequently, the graphical analysis complements our hypothesis testing and confirms our mixed results. On one side, the chart for **Maersk A, Maersk B, X-Fab, FedEx, Rockwell** and **Stadler** shows that the performance of their CAR is not strongly influenced by press releases on the cyber incident. On the other side, **Clarkson, Mondelez International, Rheinmetall, Leoni** and **Norsk Hydro** indicate a negative swing in their representative cumulated abnormal return.

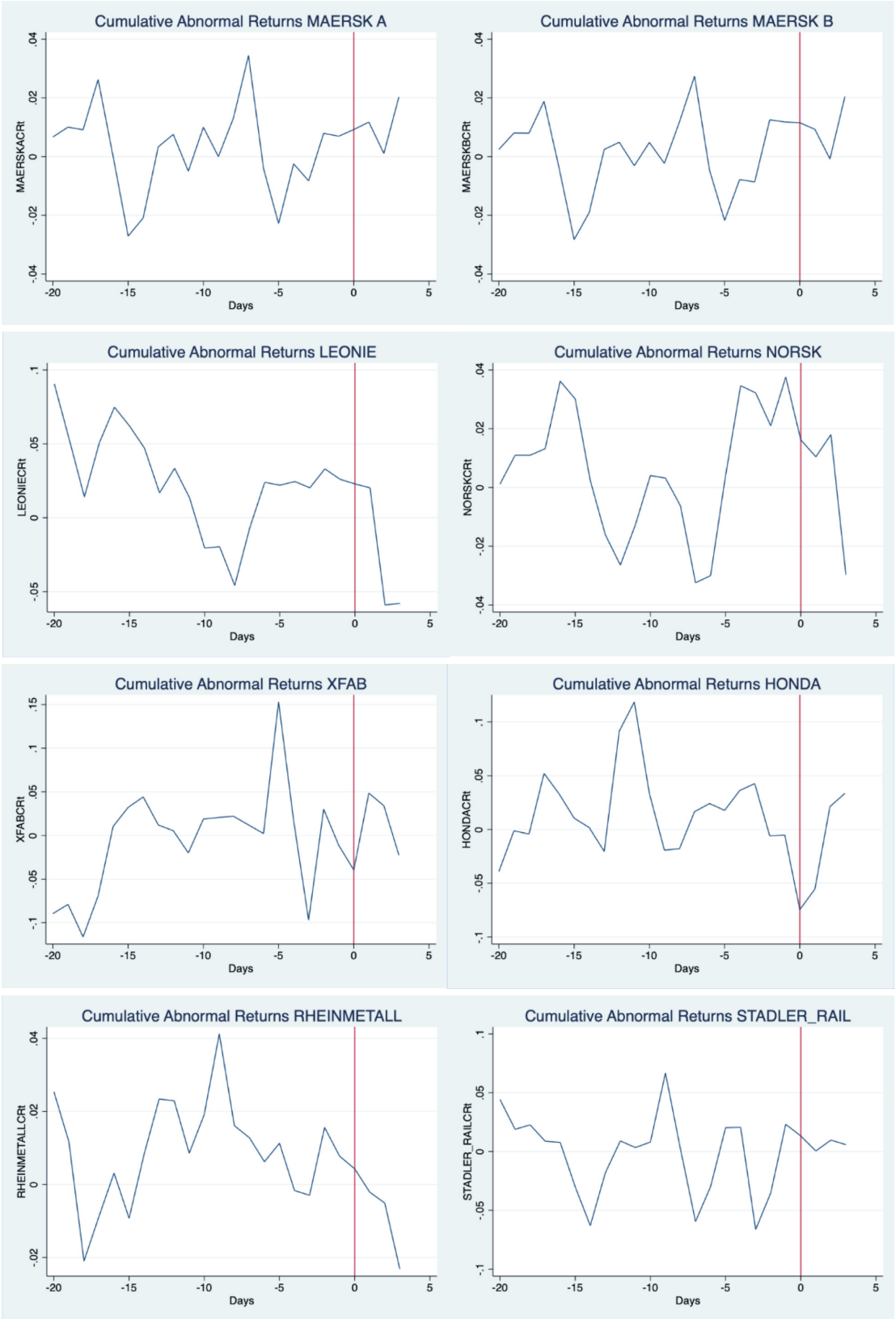
Figure 15. 100 Days – Cumulative Abnormal Returns (CAR).

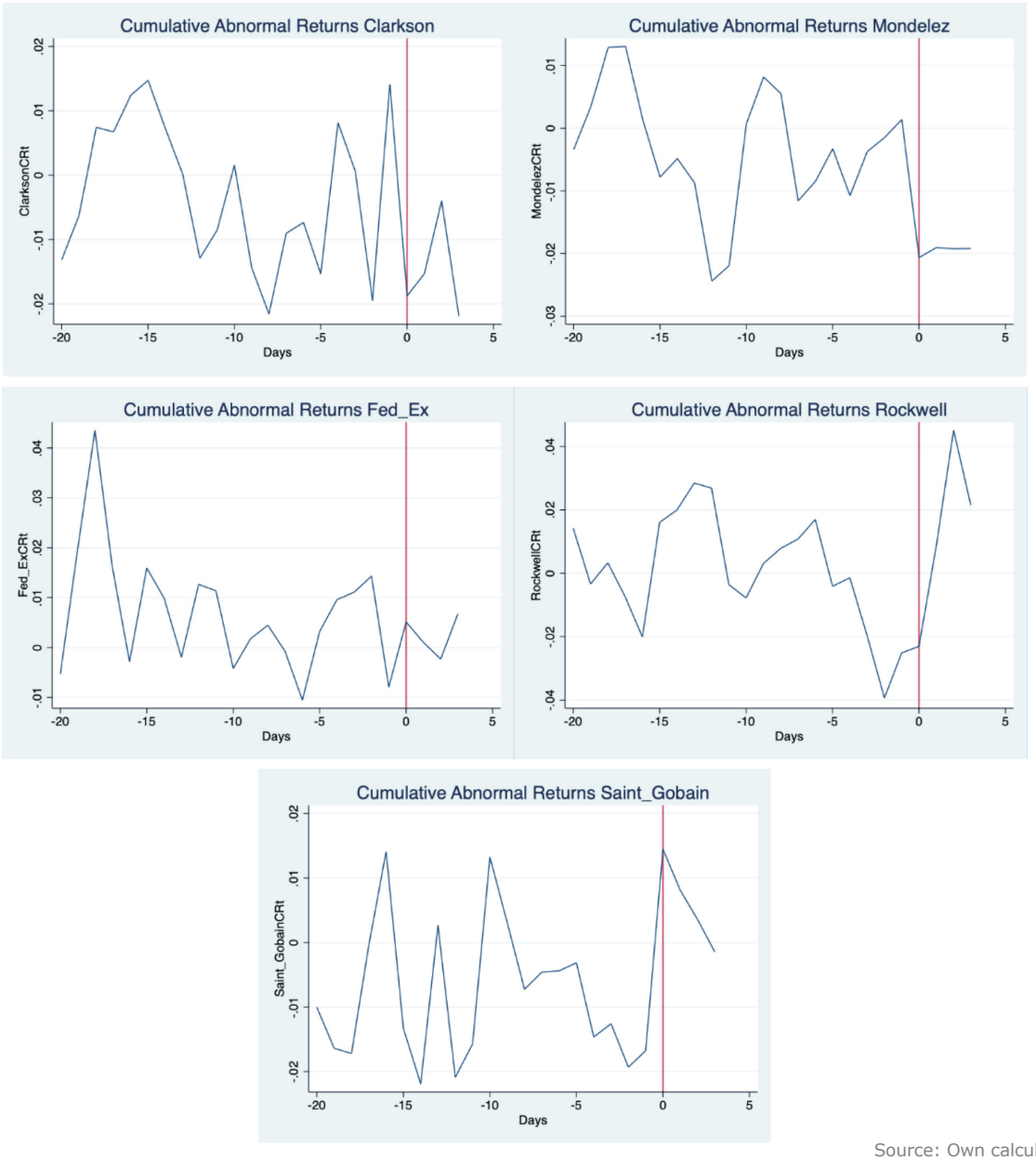




Source: Own calculations.

Figure 16. 20 Days – Cumulative Abnormal Returns (CAR).





Source: Own calculations.

In our sample, the impact of cyber incidents on stock market returns were generally small, as the results of our t-Tests indicate. The null hypothesis (H0), which states that the incident had no effect on abnormal returns, could only be ruled out for **Clarkson** and **Mondelez International** based on a 100-day estimation window. Leoni, Norsk Hydro, and Rheinmetall also showed negative effects, but not with sufficient statistical significance to rule out the null hypothesis (H0). The results for 20 days indicate that **Mondelez International, Rheinmetall,** and **Leoni** experienced abnormal returns at a significant level. The results for **Norsk Hydro** and **Clarkson** are only marginally significant, so we cannot make a clear and unambiguous statement on the relationship between cyber incidents and stock market returns here.

In general, the returns of the other stocks showed more negative effects than in the 100-day estimation period, but results are still below the level of statistical significance. In addition, we juxtaposed the results of the statistical analysis of stock returns with reported losses from annual reports (see *Table 3*) to present a broader picture of overall financial losses.

Table 3. Results Two Sample t-Test.

Company	Reported Losses	t-Test Results Mean Abnormal Return (100 days) p-value (critical value = 0.1)	t-Test Results Mean Abnormal Return (20 days) p-value (critical value = 0.1)
Maersk A	250-300 million USD according to Maersk Annual Report 2017[111]	No significant negative abnormal return 0.8288	No significant negative abnormal return 0.8468
Maersk B	250-300 million USD according to Maersk Annual Report 2017[112]	No significant negative abnormal return 0.8284	No significant negative abnormal return 0.8848
Leoni AG	40 million EUR[113]	No significant negative abnormal return 0.2685	**Significant negative abnormal return 0.0513**
Norsk Hydro	650-750 million NOK according to annual report. Company has cyber insurance[114]	No significant negative abnormal return 0.3046	Marginally significant negative abnormal return 0.1495
X-Fab	No cost data available yet; incident very recent	No significant negative abnormal return 0.6022	No significant negative abnormal return 0.6311
Honda	No cost data available yet; incident very recent	No significant negative abnormal return 0.3620	No significant negative abnormal return 0.1807
Rheinmetall	No cost data available yet; incident very recent	No significant negative abnormal return 0.2315	**Significant negative abnormal return 0.0499**
Stadler Rail	No cost data available yet; incidents very recent	No significant negative abnormal return 0.5521	No significant negative abnormal return 0.5919
Clarkson	Minimal financial damage according to annual report[115]	**Significant negative abnormal return 0.0667**	Marginally significant negative abnormal return 0.1180
Mondelez International	114 million USD[116]	**Significant negative abnormal return 0.0496**	**Significant negative abnormal return 0.0402**
FedEx	400 million USD according to FedEx Annual Report 2018[117]	No significant negative abnormal return 0.6432	No significant negative abnormal return 0.391
Rockwell Automation	No costs induced[118]	No significant negative abnormal return 0.8397	No significant negative abnormal return 0.8454
Saint-Gobain	67 million EUR[119]	No significant negative abnormal return 0.6158	No significant negative abnormal return 0.8333

Source: Own calculations.

4.1.4. The Economic Impact of Cyber Supply Chain Attacks

The psychology of markets has preoccupied financial analysts for quite some time. Predicting or identifying certain trends at an early stage is invaluable. However, certain market reactions are not always comprehensible, and thus unpredictable. This applies particularly to the influence of external effects, which can have a rapid and sometimes severe impact. Cybersecurity incidents are among these externalities that, in a perfect market,

111 See Maersk (2018).
112 See Ibid.
113 See Leoni AG (2018).
114 See Norsk Hydro (2020).
115 See Clarkson (2018).
116 See Mondelez Int. (2018).
117 See FedEx (2019).
118 See ptsecurity (2017).
119 See Saint Gobain (2018).

should elicit an immediate response. However, in the present event study, we were unable to provide substantial evidence of a generally statistically significant response to a cyber incident.

Campbell et al.[120] used a comparable methodology and reported largely insignificant results. Thus, our mixed results generally align with studies that found a strong association with stock returns after cyber incidents (Cavusoglu et al.)[121] and those that found no relationship at all (Campbell et al. 2003). The reasons for this may be manifold. Nevertheless, it can be speculated that investors have also learned from past incidents and that the nervousness on markets triggered by recurring events has eased somewhat.

Furthermore, as Cavusoglu et al.[122] note, all event studies suffer from the **assumption of information-efficient markets and rational investors**. Fama's[123] efficient market hypothesis is generally a strong and controversial assumption that also has its critiques (see for example Ball[124] for a discussion following the Lehman crash).

This is compounded by other factors such as business cyclical effects. The cyberattack on X-Fab, for example, occurred in early summer during the first COVID-19 lockdown in Germany, where the business disruption and the resulting production downtime may not have been as dramatic as one would expect in a boom year.

Moreover, reported financial losses due to the cyberattack were quite heterogeneous across companies. Rockwell Automation, for example, did not report any losses due to the incident in their annual report. Nevertheless, the results for Maersk, FedEx and Saint-Gobain are counterintuitive, as they reported massive losses.

However, limitations of our analysis include the **very small sample size** as a result of the **narrow definition** of cyber supply chain attacks, and **limited open-source data** access. A **sentiment analysis** to assess the impact of the news (on the cyber incident) itself, as a proxy for the panic factor on the market, might be a meaningful addition. Sentiment analysis is the field of research that analyses people's opinions, emotions, and feelings expressed in written form.[125]

Further research with **larger sample sizes** and **multiple methodologies** within and outside the event study framework is generally needed to examine financial losses resulting from cyber incidents, especially for companies that fall into the narrow category of intermediate suppliers.

To gain an overall perspective on economic and financial losses, it is helpful to include and compare both event studies and results from annual reports, as we did in this study. The latter conveys an impression of summarised operational and realised losses, while the former is an indicator of expectations of further financial development. Both accounting data and the analysis of stock returns are complementary, as accounting serves the purpose of reporting past profits and losses, while stock returns anticipate expectations for the future.

In addition, variables other than stock market returns should be considered for further research, such as the effect on bid-ask spreads or total trading volume, as suggested by Rosati et al.[126] Long-term investors may, for example, buy shares strategically to avoid panic sales following an event and thus counteract negative price volatility.

Overall, a more balanced approach may be achieved by collecting market data in addition to closing prices and focusing more on **market movements on the day of the event**, and in this sense also **shortening the event window**.

120 See Campbell et al. (2003): p. 443.
121 See Cavusoglu/Mishra/Raghunathan (2004): p. 94.
122 See Ibid, p. 96.
123 See Fama (1960).
124 See Ball (2009).
125 See Liu (2015).
126 See Rosati et al. (2017).

5 RECOMMENDATIONS

In systems in which more and more interfaces are created and which are increasingly harmonised, vulnerabilities are a seemingly inevitable consequence. Nevertheless, some basic practices can help to build resilience and create certain redundancies. These measures not only strengthen one's own infrastructure, but also ensure that interfaces and supply chains are examined and, as individual elements, ultimately follow a holistic approach.

In such cases, a functioning risk management system can achieve greater impact if it incorporates a holistic risk assessment by considering the following three elements or the **3Rs** of risk management:

- **Resilience:** The system ought to be adapted to potential scenarios/shocks by ensuring processes are dynamic and can be modified without losing function. This includes analysing core activities for dynamic adaption.

- **Robustness:** The system should maintain its basic functionalities under high "stress/pressure". Interfaces should be designed to resist a degree of shock.

- **Redundancy:** Components and functions of a system or infrastructure should have parallel units where they are critical, so that they can substitute them in the event of a system failure.

We have identified the following main actions:

↪ *Create an overview of own supply chains and interfaces*

The COVID-19 pandemic has shaken up supply chains around the world, exposing both dependencies and vulnerabilities. Nevertheless, the pandemic was a booster for digitalisation, and it is therefore not surprising that traditional supply chains are increasingly digitalised, creating new interfaces and thus new potential vulnerabilities.

Companies often have only limited insights into their third-party vendors' infrastructure and interfaces.[127] This, however, can increase the attack surface and malicious activities.

It is therefore indispensable that companies analyse their supply chains, dependencies, and interfaces, and perform an assessment of their hard- and software environment and update it permanently. Some companies have already lost oversight due to the multitude of interfaces and simply hope that nothing will go wrong. However, this can be neither the requirement for quality management nor for cybersecurity, which eventually jeopardises the existence of the entire company, especially that of SMEs.

↪ Overview of critical assets – especially intangible assets and indirect costs

With the development of the knowledge economy, the contribution of intangible assets to value creation has become obvious to stock-holding companies, managers, and strategists. [128] This significance is reflected in the large discrepancy between the book value of companies (the tangible assets) and the stock market value, which captures all the economic (tangible and intangible) assets of a company. Many different methods and theories have been proposed for valuing intangible assets in recent years. [129]

Regarding financial valuation, from a more pragmatic point of view, there are three main approaches to value intangible assets: the market, income, and cost method.

The market approach examines recent transactions and market prices in similar intangible assets, regardless of the type of asset being valued, and adjusts for the differences between them. When valuing real estate, for example, factors such as the unit's square footage, the age and location of the building, and its amenities may be considered.

127 See BlueVoyant (2020): p. 6.
128 See Bontis (2001).
129 See Bounfour et al. (2017).

As the market approach is based on comparisons with similar assets, extensive data on recent sales of comparable assets is essential. In practice, such comparisons are thus dependent on data quality and quantity, and are therefore prone to inaccuracies. A disadvantage of this method is that in many situations it cannot be applied due to the nature of the intangible assets. For some intangible assets, there is no active market, or they are so unique that they cannot be compared to any similar intangible assets.

The cost approach (based on the economic principle of substitution) differentiates between valuation based on reproduction costs, and valuation on the basis of replacement costs. Valuation based on reproduction costs determines the costs that would be incurred to produce a copy of the intangible asset (duplicate). A valuation based on replacement cost, on the other hand, is carried out with the aim of determining the costs that would be incurred to acquire an intangible asset that has the same functionality as another comparable asset.

The income approach is the most widely used approach for determining the value of intangible assets. The valuation must consider the amount of financial surpluses expected from the use of the intangible asset or the economic benefit that can be derived from it. In addition, it must consider how long financial surpluses are expected from the use of the intangible asset (service life). Finally, it must consider what risk exists in connection with the expected use (discount rate). The income approach determines the value of an asset by discounting the future cash flows or cost savings generated by the asset to present value. This method requires the valuation to determine the future cash flows generated by the asset, the discount rate, and the terminal value of the asset. The main difficulty lies in the separation of income from intangible assets, from income generated by non-intangible assets.

These methods help to conduct a valuation analysis in different ways and to distinguish tangible and intangible assets. However, for smaller companies, which may shy away from complex and cost-intensive valuation methods, it is helpful to roughly categorise certain types of intangible assets according to the following categories:

- reputation with clients (steady customers, customer relations/service)
- brand names
- key competences and human capital (assembled workforce, education, specific/unique skills, job tenure)
- innovation and intellectual property (patents, technology, copyrights, trade and business secrets, services)
- data (client, ecosystem, suppliers, functional data such as for HR, finance and fiscal)

Companies that do not take these valuation elements into account and assume that, even in an increasingly digital value chain, only physical assets have a relevant value, could find themselves in an existentially threatening situation in the event of an incident.

↪ Business continuity management concept: manual/guide for the procedure in a worst-case scenario

When an incident occurs, people often panic when whole systems or even entire infrastructures are affected, making work impossible. In such cases, a business continuity management concept sets a framework for key personnel to ensure that everyone knows which measures are required in their area of responsibility to limit the impact. This includes the clear allocation of responsibilities (of people in general, but also responsibilities on holidays, weekends, and outside normal business hours); the consideration of technical and organisational aspects of the company; the internal and external communication with authorities, insurance companies, the police, customers, suppliers, and other business partners, employees and supporting units such as cybersecurity companies; and the implementation of a protocol that defines how to deal with various events.

The exchange with other companies, especially those that have already been affected and have been able to gain experience, can be helpful. This also includes cybersecurity authorities, the own insurance, interest groups, cities and municipalities, and researchers in the field. These best practices are a guideline that must be adapted to the company's own needs. In addition, so-called penetration tests can also help to test the digital channels to the outside world and identify vulnerabilities at an early stage.

Regardless of the individual security measure and the budget, it is important to deal with this issue. It is important to consider the consequences of a digital or even physical attack on individual areas and on the entire system. This is the best strategy for identifying potential vulnerabilities and reducing the risk of unpleasant surprises. In addition, some past cases show that customers appreciate transparency and good crisis management, even if they themselves are affected by the incident.[130]

However, if taken completely by surprise, companies can quickly find themselves in chaos and ultimately in a situation that threatens the very existence of the company.

⮑Problem of lack of transparency and willingness to share data with other business partners

While on the one hand companies often lack a clear overview of the interfaces and interconnections with suppliers, business partners, and regular customers, on the other hand they are often also unwilling to share their experiences from past cyber incidents with third parties. This is often justified by data protection regulations, fear of reputational damage, staff shortages, and the like. However, transparency is also important for those who have already been affected, as it creates trust and because incidents can recur in this dynamic environment.

A network of like-minded peers benefits all parties involved as patterns repeat, and thus may prevent others from falling into the same trap. Moreover, best practices can have a more far-reaching impact and investments can be scaled (for example group certification in IT security standards and purchasing power for software and hardware for IT- and cybersecurity).

Interest groups can not only gain more economic weight through a merger, but also political weight. They become more visible, can point out problems and vulnerabilities, and apply constructive leverage on decision-makers.

Dealing with incidents transparently is not a sign of weakness, but shows strength by addressing challenges openly and sharing experiences in the industry. Only through cooperation and knowledge sharing can vulnerabilities be reduced, and cybersecurity increased. However, this is a mindset and not a one-time project.

⮑Cyber insurance can contribute to a higher general level of IT security

Cyber insurance allows a company to protect itself against the financial consequences of a cyber incident. It transfers the residual risk to an insurer and thus makes it possible in the first instance to take certain risks of digitalisation in an entrepreneurially responsible manner. For the insurer, the risk becomes more calculable through scaling, which is an incalculable coincidence for the individual company. In this context, cyber insurance should be seen as an element of IT risk management and should in no way replace investments in IT security.

That is the theory. However, past events have shown that many customers of an insurer can be affected at the same time, which can lead to considerable financial burdens for the insurance company. On the other hand, insurers try to exclude more and more covers, which can lead to ambiguities for policyholders and to high financial risk in the case of a high claim that is not covered or only partially covered.

Most insurance companies have moved towards requiring certain IT and cybersecurity standards, without which policies will not be issued. Thus, insurers become de facto regulators, as they set standards for the issuance of an insurance policy.

130 Becker's Health IT (2015).

6 CONCLUSION

This study examined the economic costs of cyber operations targeting supply chains from two perspectives: by performing an analysis of stock market data with the event study methodology to estimate the costs of cyber supply chain attacks, and by conducting two in-depth case studies.

The event study did not provide substantial evidence of a general statistically significant response to cyber incidents in equity markets. The rather mixed results, however, are generally consistent with studies that indicated a strong association with stock returns following a cyber incident, and those that found no connection at all. Yet event studies suffer from the assumption of information-efficient markets and rational investors, which are nowadays controversial due to recent developments such as the financial crisis in 2008, the COVID-19 pandemic, and the recent war in Ukraine.

Limitations of our analysis include the very small sample size due to the narrow definition of CSCAs, and limited access to open source data. To examine financial losses resulting from cyber incidents, further research with larger sample sizes and multiple methodologies within and outside the scope of event studies is generally needed, especially for companies that fall into the narrow category of third-party vendors.

In the Kaseya case study, we highlighted how a critical supplier can be massively obstructed in its business, which may affect the entire MSPs sector as a distributed attack. However, although Kaseya has not yet indicated whether it has suffered significant financial damage, the damage could be vast. Kaseya's customers are largely MSPs, who are themselves responsible for approximately 800,000 to one million small and local businesses worldwide. Thus, the tangible as well as intangible damage may be significant, as not only direct but also substantial indirect costs may have been incurred by the company and its customers.

In the SolarWinds case study, we highlighted how attackers can exploit supply chains to achieve their ultimate objective. While the actual financial damage of the SolarWinds breach was huge in itself – more than $27 million – there is another serious asset that is damaged by such attacks: the trust between the supplier and the company, particularly in areas such as security and software management. A loss of trust can result in a customer churn and, in the worst case scenario, bankruptcy.

The CSCA on various organisations via updates of SolarWinds' Orion software illustrates once again how vulnerable inadequately secured links in supply chains are and how they present a giant gateway for malicious activities. In particular when suppliers have administrative system access, the door is left open for attackers. Supply chain attacks are not a new phenomenon, but due to the proliferation of networking and the creation of new interfaces, the risks are mounting, and vulnerability remains high. There is thus still increased need for research that addresses the financial consequences to provide a distinct assessment of the overall impact.

The cyber domain is extremely dynamic, forcing both attackers and defenders to evolve constantly. On the one hand, cyber insurance, PR, and crisis management as well as general awareness on the part of companies and investors may favour smooth market reactions to incidents. On the other hand, the overall level of connectivity and reliance on information technologies is increasing, and with it the value of data and digital access in general. This, however, also raises the stakes of an incident and the potential impact on the reputation of the organisation.

Hence, the aim of this study was to quantify the damage of cyber incidents for companies by applying an econometric analysis and to illustrate it in two case studies for targeted and distributed attacks. Even if the results of the impact on listed companies are not unambiguous at first glance, losses can be significant, as some of the analysed annual reports clearly show. Thus, with this study we want to create more awareness for the risks that arise for companies that are part of a supply chain and support their risk analysis with concrete figures and potential actions.

The global economy has created a greater attack surface through an ever increasing number of interfaces, of which many companies are not aware. These vulnerabilities can have different levels of complexity. However, companies can already identify potential risks by simple means, such as by conducting an assessment of their interfaces and their own critical assets, and thus address them more effectively.

In our recommendations we formulate initial, rather basic measures that must be tailored to individual needs and should ideally be supported by experts. Risk management starts with an assessment, but does not end there. Once awareness has been established, ideally not on an incident-related level, the necessary investments are easier to justify and measures easier to priorities.

Consequently, our study covered both case-specific and more generic approaches to analysis, providing a broad perspective on the subject. A further research avenue should combine these approaches to support building a more holistic view of ecosystems and their evolution from both a business opportunity and cyber risk perspective.

REFERENCES

Andersson, Alexander (2021), How the Kaseya VSA Zero Day Exploit Worked, in: Truesec, URL: https://www.truesec.com/hub/blog/kaseya-vsa-zero-day-exploit, [17.05.2022].

Ball, Ray/Brown, Philip (1968): An Empirical Evaluation of Accounting Income Numbers. Journal of Accounting Research, 6(2): 159-178.

Ball, Ray (2009): The global financial crisis and the efficient market hypothesis: what have we learned?. Journal of Applied Corporate Finance, 21(4), 8-16.

Beaver, William H. (1968). The information content of annual earnings announcements, Journal of accounting research, 67-92.

Becker‘s Health IT (2015): Consumer perceptions of Anthem slightly shift downward following data breach, URL: https://www.beckershospitalreview.com/healthcare-information-technology/consumer-perceptions-of-anthem-slightly-shift-downward-following-data-breach.html, [20.05.2022].

Belkind, Leonid (2019): Think Your Supply Chain is Truly Secure? Think Again, in: Symantec Enterprise Blogs, URL: https://symantec-enterprise-blogs.security.com/blogs/feature-stories/think-your-supply-chain-truly-secure-think-again?om_ext_cid=biz_social3_AMS_NAM-US_twitter_us,blogs-social,FY20-Q1,Blog,Blog%20Feature%20Stories,org, [10.12.2020].

Bing, Christopher (2020): Suspected Russian hackers spied on U.S. Treasury emails – sources, in: Reuters, URL: https://www.reuters.com/article/us-usa-cyber-amazon-com-exclsuive/exclusive-u-s-treasury-breached-by-hackers-backed-by-foreign-government-sources-idUSKBN28N0PG, [17.05.2022].

Bing, Christopher/Stubbs, Jack/Satter/Menn (2021): Exclusive: Suspected Chinese hackers used SolarWinds bug to spy on U.S. payroll agency – sources, in: Reuters, URL: https://www.reuters.com/article/us-cyber-solarwinds-china-exclusive/exclusive-suspected-chinese-hackers-used-solarwinds-bug-to-spy-on-u-s-payroll-agency-sources-idUSKBN2A22K8, [11.04.2022].

BlueVoyant (2020). Global Insights: Supply Chain Cyber Risk – Managing Cyber Risk Across the Extended Vendor Ecosystem, URL: https://www.bluevoyant.com/resources/managing-cyber-risk-across-the-extended-vendor-ecosystem, p. 8.

Brown, Stephen/Warner, Jerold (1985): Using Daily Stock Returns. The Case of Event Studies, Journal of Financial Economics, 14 (1985), 3-31. North-Holland.

Bontis, Nick (2001): Assessing Knowledge Assets: A Review of the Models Used to Measure Intellectual Capital. International Journal of Management Reviews 3 (1): 41–60.

Bounfour, Ahmed (2003): The Management of intangibles, The organisation’s Most Valuable Assets. Routledge, London.

Bounfour, Ahmed/Ozaygen, Altay/Dieye, Rokhaya/Szanto, Alexander/Kammoun, Niaz (2017): Generic model of intangibles cyber-risks , URL: https://www.hermeneut.eu/wp-content/uploads/2018/08/HERMENEUT-D3.1-Generic-model-of-intangibles-cyber-risks.pdf.

Boyens, Jon/Smith, Angela/Bartol, Nadya/Winkler, Kris/Holbrook, Alex/Fallon, Matthew (2022): Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations Special, in: NIST Special Publication, Publication NIST SP 800-161r1, URL: https://doi.org/10.6028/NIST.SP.800-161r1, [17.05.2022].

Byran, Jordan (2019): A Better Way to Manage Third-Party Risk, in: Gartner, URL: https://www.gartner.com/smarterwithgartner/a-better-way-to-manage-third-party-risk/, [10.03.2022].

Camp, Cameron/Goretsky, Aryeh (2021): Kaseya supply-chain attack: What we know so far, in: welivesecurity, URL: https://www.welivesecurity.com/2021/07/03/kaseya-supply-chain-attack-what-we-know-so-far/, [17.05.2022].

Campbell, Katherine/Gordon, Lawrence A./Loeb, Martin P./Zhou, Lei (2003): The economic cost of publicly announced information security breaches: empirical evidence from the stock market, Journal of Computer Security, 11(3), 431–448.

Carlson, Kara (2021): Austin‘s SolarWinds spins off business unit into new company, N-able, in: Austin American Statesman, URL: https://eu.statesman.com/story/business/2021/07/20/solarwinds-spinoff-leads-formation-new-company-n-able/8017235002/, [11.04.2022].

Cavusoglu, Huseyin/Mishra, Birendra/Raghunathan, Srinivasan (2004): The effect of internet security breach announcements on market value: Capital market reactions for breached firms and internet security developers. International Journal of Electronic Commerce, 9(1), 70–104.

Clarkson (2018): Rethinking Our Industry: Clarkson PLC Annual Report 2017, URL: https://www.clarksons.com/media/1137918/ckn_annual_report_2017.pdf, [17.05.2022].

Comeau, Zachary (2021): SolarWinds Expects Cyber Incident Costs Up To $25 Million in 2021, in: My Tech Decision, URL: https://mytechdecisions.com/it-infrastructure/solarwinds-cyber-incident-costs/, [17.05.2022].

Cybereason (2021): Organizations at risk: ransomware Attackers don’t take holidays, in: Cybereason, URL: https://www.cybereason.com/ransomwareattacksdonttakeholidays/webinar/us/12121, [17.05.2022].

Cybersecurity and Infrastructure Security Agency (2020): Emergency Directive 21-01-Mitigate SolarWinds Orion Code Promise, URL: https://cyber.dhs.gov/ed/21-01/, [11.04.2022].

Cybersecurity and Infrastructure Security Agency (2021a): Joint Statement by the Federal Bureau of Investigation (FBI), the Cybersecurity and Infrastructure Security Agency (CISA), the Office of the Director of National Intelligence (ODNI), and the National Security Agency (NSA), URL: https://www.cisa.gov/news/2021/01/05/joint-statement-federal-bureau-investigation-fbi-cybersecurity-and-infrastructure, [17.05.2022].

Cybersecurity and Infrastructure Security Agency (2021b): CISA and FBI urge organizations to remain vigilant to ransomware threats on holidays, including this labor day, URL: https://www.cisa.gov/news/2021/08/31/cisa-and-fbi-urge-organizations-remain-vigilant-ransomware-threats-holidays, [17.05.2022].

Cybersecurity and Infrastructure Security Agency (2022): Alert (AA22-131A). Protecting Against Cyber Threats to Managed Service Providers and their Customers, URL: https://www.cisa.gov/uscert/ncas/alerts/aa22-131a, [16.05.2022].

Dumontier, Pascal/Martinez, I. (2001): “Les Études d’Événements en Comptabilité Financière.” Faire de la Recherche en Comptabilité Financière, éds. P. Dumontier et R. Teller. Paris, Vuibert: 103-115.

Dunleavy, Jerry (2020): National Security Council sets up coordinated government response to SolarWinds hack, in: Washington Examiner, URL: https://www.washingtonexaminer.com/

REFERENCES

news/national-security-council-coordinated-government-response-solarwinds-hack, [17.05.2022].

ESET Research (2021): Tweet, in: Twitter, URL: https://twitter.com/ESETresearch/status/1411541353889153026, [17.05.2022].

European Union Agency for Cybersecurity [ENISA] (2021): ENISA Threat Landscape for Supply Chain Attacks, URL: https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks/@@download/fullReport, p. 3.

Fama, Eugene F. (1960): Efficient market hypothesis (Doctoral dissertation, Ph. D. dissertation, University of Chicago, Graduate School of Business).

Fama, Eugene F./Fisher, Lawrence/Jensen/Roll (1969): The Adjustment of Stock Prices to New Information. International Economic Review, 10(1): 1-21.

Fama, Eugene F. (1991): Efficient Capital Markets: II, The Journal of Finance, Vol. 46 No. 5, pp. 1575-1617.

FedEx (2019): Annual Report 2018, URL: https://s21.q4cdn.com/665674268/files/doc_financials/annual/2018/FedEx-Annual-Report-2018.pdf, [17.05.2022]

Finnegan, Conor/Nagle, Molly (2021): In hour-long call, Biden discusses ransomware with Putin after another massive attack, in: ABC News, URL: https://abcnews.go.com/Politics/hour-long-call-biden-discusses-ransomware-putin-massive/story?id=78761441, [17.05.2022].

FireEye (2020): Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims With SUNBURST Backdoor, in: Mandiant, URL: https://www.mandiant.com/resources/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor, [17.05.2022].

Fraunhofer-Institut für Kommunikation, Informationsverarbeitung und Ergonomie [FKIE] (2021): Cobalt Strike, URL: https://malpedia.caad.fkie.fraunhofer.de/details/win.cobalt_strike, [17.05.2022].

Gevers, Victor (2021): Kaseya case update 2, in:DIVD CSIRT, URL: https://csirt.divd.nl/2021/07/04/Kaseya-Case-Update-2/, [17.05.2022].

Gordon, Lawrence A./Loeb, Martin P./Zhou Lei (2011): The Impact of Information Security Breaches: Has There Been a Downward Shift in Costs?, Journal of Computer Security, Vol. 19 (1), pp. 33-56.

Greig, Jonathan (2021a): REvil websites down after governments pressured to take action following Kaseya attack, in: ZDNet, URL: https://www.zdnet.com/article/revil-websites-down-after-governments-pressured-to-take-action-following-kaseya-attack/, [17.05.2022].

Greig, Jonathan (2021b): Kaseya denies paying ransom for decryptor, refuses comment on NDA, in: ZDNet, URL: https://www.zdnet.com/article/kaseya-denies-paying-ransom-for-decryptor-refuses-comment-on-nda/, [17.05.2022].

Harrell, Barry (2011): Fast-growing Austin software maker Solarwinds acquires Idaho company, in: Statesman, URL: https://web.archive.org/web/20180124071125/http://www.statesman.com/business/fast-growing-austin-software-maker-solarwinds-acquires-idaho-company/tNaIxy1wxM0gek655LmPqN/, [17.05.2022].

Harwell, Drew/MacMillian, Douglas (2020): Investors in breached software firm SolarWinds traded $280 million in stock days before hack was revealed, in: Washington Post, URL: https://www.washingtonpost.com/technology/2020/12/15/solarwinds-russia-breach-stock-trades/, [17.05.2022].

Hjelmvik, Erik (2021): Twenty-three SUNBURST Targets Identified, in: NETRESEC, URL: https://www.netresec.com/?page=Blog&month=2021-01&post=Twenty-three-SUNBURST-Targets-Identified, [20.05.2022].

Identity Theft Resource Center [ITRC] (2021): Third Quarter 2021 Data Breach Analysis, URL: https://itrc--c.na151.content.force.com/file-asset-public/ITRC_2021_Q3DataBreachAnalysis_Report?oid=00D300000006Kp5EAE, [30.04.2022].

IronNet (2021): Russia, ransomware, and the REvil shutdown - what does it all mean?, in:IronNet, URL: https://www.ironnet.com/blog/russias-ransomware-and-revil-shutdown, [17.05.2022].

Johnson, Katanga (2021): SEC probing SolarWinds clients over cyber breach disclosures, in: FOX Business, URL: https://www.foxbusiness.com/technology/us-sec-probing-solarwinds-clients-over-cyber-breach-disclosures-sources, [11.04.2022].

Kannan, Karthik/Rees, Jackie/Sridhar, Sanjay (2007): Market Reaction to Information Security Breach Announcements: An Empirical Analysis, International Journal of Electronic Commerce, Vol. 12(1), pp. 69-91.

Kaseya (2021a): Kaseya Home, URL: https://www.kaseya.com/, [20.05.2022].

Kaseya (2021b): Kaseya Responds Swiftly to Sophisticated Cyberattack, Mitigating Global Disruption to Customers, in: Press Release, URL: https://www.kaseya.com/press-release/kaseya-responds-swiftly-to-sophisticated-cyberattack-mitigating-global-disruption-to-customers/, [17.05.2022].

Kaseya (2021c): Updates Regarding VSA Security Incident, URL: https://www.kaseya.com/potential-attack-on-kaseya-vsa/, [17.05.2022].

Kovacs, Eduard (2021a): CISA Says Many Victims of SolarWinds Hackers Had No Direct Link to SolarWinds, in: SecurityWeek, URL: https://www.securityweek.com/cisa-says-many-victims-solarwinds-hackers-had-no-direct-link-solarwinds, [16.05.2022].

Kovacs, Eduard (2021b): Class Action Lawsuit Filed Against SolarWinds Over Hack, in: SecurityWeek, URL: https://www.securityweek.com/class-action-lawsuit-filed-against-solarwinds-over-hack, [17.05.2022].

Kritzman, Mark P. (1994): What practitioners need to know about event studies, Financial Analysis Journal, Vol 17 (20).

Leoni AG (2018): Annual Report 2017, URL: https://publications.leoni.com/fileadmin/corporate/publications/reports/2017/annual_report_2017.pdf?1521539767, [17.05.2022].

Liu, Bing (2015). Opinions, Sentiment, and Emotion in Text. Cambridge University Press.

Maersk (2018): Annual Report 2017, URL: https://investor.maersk.com/static-files/250c3398-7850-4c00-8afe-4dbd874e2a85, [17.05.2022].

Mandia, Kevin (2020): FireEye Shares Details of Recent Cyber Attack, Actions to Protect Community, in: FireEye Stories Blog, URL: https://www.fireeye.com/blog/products-and-services/2020/12/fireeye-shares-details-of-recent-cyber-attack-actions-to-protect-community.html, [19.05.2022].

McHugh, Marian (2021): Kaseya boss: ‚We'll be a public company in Q4 this year', in: CRN UK, URL: https://www.channelweb.co.uk/news/4025943/kaseya-boss-public-company-q4, [19.05.2022].

Mendrez, Rodel/Kazymirskyi, Nikita (2021): Diving Deeper Into the Kaseya VSA Attack: REvil Returns and Other Hackers Are Riding Their Coattails, in: Trustwave, URL: https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/diving-deeper-into-the-kaseya-vsa-attack-revil-returns-and-other-hackers-are-riding-their-coattails/, [17.05.2022].

Microsoft (2020): Analyzing Solorigate, the compromised DLL file that started a sophisticated cyberattack, and how Microsoft Defender helps protect customers, in: Microsoft Security, URL: https://www.microsoft.com/security/blog/2020/12/18/analyzing-solorigate-the-compromised-dll-file-that-started-a-sophisticated-cyberattack-and-how-microsoft-defender-helps-protect/, [17.05.2022].

Microsoft (2021a): Deep dive into the Solorigate second-stage activation: From SUNBURST to TEARDROP and Raindrop, in: Microsoft Security, URL: https://www.microsoft.com/security/blog/2021/01/20/deep-dive-into-the-solorigate-second-stage-activation-from-sunburst-to-teardrop-and-raindrop/, [10.05.2022].

Microsoft (2021b): Microsoft Internal Solorigate Investigation – Final Update, in: Microsoft Security Response Center, URL: https://msrc-blog.microsoft.com/2021/02/18/microsoft-internal-solorigate-investigation-final-update/, [11.05.2022].

Mondelez Int. (2018): Annual Report 2017, URL: https://ir.mondelezinternational.com/static-files/e718084d-3c92-4387-bd04-38b56b6c75e1, [20.05.2022].

Morse, Dale (1984). An Econometric Analysis of the Choice of Daily Versus Monthly Returns in Tests of Information Content, Journal of Accounting Research, Autumn, 1984, Vol. 22, No. 2 (Autumn, 1984), pp. 605-623.

N-able (2022): State of the Market: The New Threat Landscape. Pushing MSP security to the next level, URL: https://www.n-able.com/it/resources/state-of-the-market-the-new-threat-landscape, [17.05.2022].

Norsk Hydro (2020): Annual Report, URL: https://www.hydro.com/Document/Index?name=Annual%20report%202019%20web.pdf&id=506433, [05.04.2022].

Orange (2021): Winds of change: Underlying Causes and Implications of the SolarWinds attack, in: Orange Cyberdefense, p. 7.

Osborne, Charlie (2021): Updated Kaseya ransomware attack FAQ: What we know now, in: ZDNet, https://www.zdnet.com/article/updated-kaseya-ransomware-attack-faq-what-we-know-now/, [11.04.2022].

Paganini, Pierluigi (2021): Coop supermarket closes hundreds of stores after Kaseya supply chain ransomware attack, in: Security Affairs, URL: https://securityaffairs.co/wordpress/119663/cyber-crime/coop-supermarket-kaseya-ransomware-attack.html, [11.04.2022].

Panettieri, Joe (2020): Hackers Weaponize SolarWinds Orion for Worldwide Cyberattacks, in: MSSP Alert, URL: https://www.msspalert.com/cybersecurity-news/solarwinds-orion-vulnerability-investigation/, [17.05.2022].

Peterson Pamela P. (1989): Event studies: a review of issues and methodology. Quarterly Journal of Business and Economics, 28(3): 36-66.

Pirounias, Sotirios/Mermigas, Dimitrios/Patsakis (2014): The relation between information security events and firm market value, empirical evidence on recent disclosures: An extension of the GLZ study, Journal of Information Security and Applications, 19(4), 257–271.

Poulsen, Kevin/McMillan, Robert/Volz (2020): SolarWinds Hack Victims: From Tech Companies to a Hospital and University, in: The Wall Street Journal, URL: https://www.wsj.com/articles/solarwinds-hack-victims-from-tech-companies-to-a-hospital-and-university-11608548402, [11.04.2022].

ptsecurity (2017): Vulnerabilities in Rockwell Automation controllers found by Positive Technologies, URL: https://www.ptsecurity.com/ww-en/about/news/vulnerabilities-in-rockwell-automation-controllers-found-by-positive-technologies/, [11.04.2022].

Ramakrishna, Sudhakar (2021a): New Findings From Our Investigation of SUNBURST, in: orangematter, URL: https://orangematter.solarwinds.com/2021/01/11/new-findings-from-our-investigation-of-sunburst/, [17.05.2022].

Ramakrishna, Sudhakar (2021b): Our Plan for a Safer SolarWinds and Customer Community, in: orangematter, URL: https://orangematter.solarwinds.com/2021/01/07/our-plan-for-a-safer-solarwinds-and-customer-community/, [17.05.2022].

Reed, M./Miller, John F./Popick, P. (2014): Supply Chain Attack Patterns: Framework and Catalog. Office of the Deputy Assistant Secretary of Defense for System Engineering. MITRE Technical Report.

Rosati, Pierangelo/Cummins, Mark/Deeney, Peter/Gogolin, Fabian/van der Werff, Lisa/Lynn, Theo (2017): The effect of data breach announcements beyond the stock price: Empirical evidence on market activity. International Review of Financial Analysis, 49, 146-154.

Saint Gobain (2018): Annual Report 2017, URL: https://www.saint-gobain.com/sites/sgcom.master/files/comptes_conso_31-12-2017_eng.pdf, [17.05.2022].

Satter, Raphael/Bing, Christopher/Menn (2020): Hackers used SolarWinds' dominance against it in sprawling spy campaign, in: Reuters, URL: https://www.reuters.com/article/global-cyber-solarwinds/hackers-at-center-of-sprawling-spy-campaign-turned-solarwinds-dominance-against-it-idUSKBN28P2N8, [11.04.2022].

Schmidt, Jürgen (2021): Kaseya-Angriff: Cybercrime-Erpresser fordern 70 Millionen US-Dollar, in: Heise, URL: https://www.heise.de/news/Kaseya-Angriff-Cybercrime-Erpresser-fordern-70-Millionen-US-Dollar-6128705.html, [03.05.2022].

Shah, Samit (2021): The Financial Impact of SolarWinds, in: Bitsight, URL: https://www.bitsight.com/blog/the-financial-impact-of-solarwinds-a-cyber-catastrophe-but-insurance-disaster-avoided, [03.05.2022].

Sinanaj, Griselda/Zafar, Humayun (2016): Who Wins in a Data Breach? - A Comparative Study on the Intangible Costs of Data Breach Incidents, PACIS 2016 Proceedings, 60.

Smith, Brad (2020): A moment of reckoning: the need for a strong and global cybersecurity response, in: Microsoft On the Issues, URL: https://blogs.microsoft.com/on-the-issues/2020/12/17/cyberattacks-cybersecurity-solarwinds-fireeye/, [11.04.2022].

REFERENCES

SolarWinds (2020a): Tweet, in: Twitter, URL: https://twitter.com/solarwinds/status/1338325699300651018, [20.05.2022].

SolarWinds (2020b): Q4'20 Results, URL: https://s22.q4cdn.com/673701899/files/doc_financials/2020/q4/SolarWinds-Q4‘20-Earnings-Call-Presentation_vf.pdf, [20.05.2022].

SolarWinds (2021a): Investor Relations, URL: https://investors.solarwinds.com/overview/default.aspx, [17.05.2022].

SolarWinds (2021b): About SolarWinds, URL: https://www.solarwinds.com/company/home, [17.05.2022].

SolarWinds (2021c): News, URL: https://investors.solarwinds.com/news/default.aspx, [17.05.2022].

SolarWinds (2021d): Quarterly Results, URL: https://investors.solarwinds.com/financials/quarterly-results/default.aspx, [20.05.2022].

Symantec (2018): New Orangeworm attack group targets the healthcare sector in the U.S., Europe, and Asia, URL: https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/orangeworm-targets-healthcare-us-europe-asia, [10.12.2020].

Symantec (2019): Internet Security Threat Report, URL: https://docs.broadcom.com/doc/istr-24-2019-en, p. 17, [10.12.2020].

Symantec (2021): Raindrop: New Malware Discovered in SolarWinds Investigation, in: Symantec Enterprise Blogs, URL: https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/solarwinds-raindrop-malware, [11.04.2022].

Szanto, Alexander (2019). White paper on cybercrime and cyberterrorism, Finance.

Temple-Raston, Dina (2021): A ‚Worst Nightmare' Cyberattack: The Untold Story Of The SolarWinds Hack, in: NPR, URL: https://www.npr.org/2021/04/16/985439655/a-worst-nightmare-cyberattack-the-untold-story-of-the-solarwinds-hack, [17.05.2022].

The White House (2016): Presidential Policy Directive -- United States Cyber Incident Coordination, in: the White House, URL: https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident, [17.05.2022].

The White House (2021a): FACT SHEET: Imposing Costs for Harmful Foreign Activities by the Russian Government, in: the White House, URL: https://www.whitehouse.gov/briefing-room/statements-releases/2021/04/15/fact-sheet-imposing-costs-for-harmful-foreign-activities-by-the-russian-government/, [11.04.2022].

The White House (2021b): Executive Order on Improving the Nation's Cybersecurity, in: the White House, URL: https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/, [17.05.2022].

Thomas, Brian (2020): FBI Alerts Companies of Cyber Attacks Aimed at Supply Chains, Bitsight, URL: https://www.bitsight.com/blog/fbi-alerts-companies-of-cyber-attacks-supply-chains, [10.03.2022].

Tucker, Eric (2020): Senator: Treasury Dept. email accounts compromised in hack, in: Associated Press, URL: https://apnews.com/article/technology-politics-ron-wyden-russia-hacking-572ac201e8f365cf6ec218b478742aa0, [17.05.2022].

Tucker, Eric (2021): Hackers targeted SolarWinds earlier than previously known, in: Associated Press, URL: https://apnews.com/article/hacking-business-technology-government-and-politics-b221968496ed498457ab56aae7970c90, [11.04.2022].

United States Securities and Exchange Commission (2018): Commission Statement and Guidance on Public Company Cybersecurity Disclosures, in: Securities and Exchange Commission, URL: https://www.sec.gov/rules/interp/2018/33-10459.pdf, [17.05.2022].

United States Securities and Exchange Commission (2020): SEC Report CIK #0001739942, URL: https://www.sec.gov/ix?doc=/Archives/edgar/data/1739942/000162828020017451/swi-20201214.htm, [11.04.2022].

United States Senate (2020): Letter to CISA and FBI regarding SolarWinds, URL: https://www.moran.senate.gov/public/_cache/files/e/d/ed2078ad-8f58-460a-ab54-5ffe570bfd23/9E2CFEA30538117FF470015EBAD88368.12.15.2020---letter-to-cisa-and-fbi-re-solarwinds---final-signed.pdf, [17.05.2022].

U.S. Department of Justice (2021): Ukrainian Arrested and Charged with Ransomware Attack on Kaseya, in: Justice News, URL: https://www.justice.gov/opa/pr/ukrainian-arrested-and-charged-ransomware-attack-kaseya, [11.04.2022].

Vaughan-Nichols, Steven J. (2021): SolarWinds security fiasco may have started with simple password blunders, in: ZDNet, URL: https://www.zdnet.com/article/solarwinds-security-fiasco-may-have-started-with-simple-password-blunders/, [20.05.2022].

Viggiani, Fabio (2020): The SolarWinds Orion SUNBURST Supply Chain Attack, in: Truesec, URL: https://www.truesec.com/hub/blog/the-solarwinds-orion-sunburst-supply-chain-attack, [17.05.2022].

Viggiani, Fabio (2021): Kaseya Supply-Chain Attack Targeting MSPs to Deliver REvil Ransomware, in: Truesec, URL: https://www.truesec.com/hub/blog/kaseya-supply-chain-attack-targeting-msps-to-deliver-revil-ransomware, [17.05.2022].

Volz, Dustin/McMillan, Robert (2020): Suspected Russian Hack Said to Have Gone Undetected for Months, in: The Wall Street Journal, URL: https://www.wsj.com/articles/suspected-russian-hack-said-to-have-gone-undetected-for-months-11607974376?mod=tech_lead_pos3, [17.05.2022].

Weinert, Alex (2021), Using Zero Trust principles to protect against sophisticated attacks like Solorigate, in: Microsoft Security, URL: https://www.microsoft.com/security/blog/2021/01/19/using-zero-trust-principles-to-protect-against-sophisticated-attacks-like-solorigate/, [17.05.2022].

Yahoo!Finance (2021): SolarWinds Corporation (SWI) Stock Chart, in: yahoo!finance, URL: https://finance.yahoo.com/quote/SWI?p=SWI&guccounter=1, [17.05.2022].

Yayla, Ali Alper/Hu Qing (2011): The Impact of Information Security Events on the Stock Value of Firms: The Effect of Contingency Factors, Journal of Information Technology, Vol. 26(1), pp. 60-77.

ABOUT THE AUTHORS

Esther Kern joined BIGS in August 2019 as a Research Fellow. She works in national as well as European projects on various societal, security policy and economic issues related to technology and security. Her research focuses on particular on cyber and space security. In her bachelor's degree, Esther studied political science and history at the Albert-Ludwigs-Universität Freiburg and in Connecticut, US. Subsequently, she earned her master's degree in North American Studies at the John-F.-Kennedy-Institute at Freie Universität Berlin with a focus on foreign and security policy. Esther gained first working experiences among others at Stiftung Wissenschaft und Politik – German Institute for International and Security Affairs and the American Institute for Contemporary German Studies in Washington D.C. Prior to joining BIGS, she worked as a project manager for an European election campaign.

Alexander Szanto joined BIGS in May 2017 as a Research Fellow and is working in national and EU projects on various economic, societal and security policy related aspects of cybersecurity. Alexander graduated from the University of Maastricht with a European Studies Bachelor's degree, with a semester abroad in International Relations at the Institut d'études politiques (Sciences Po) in Paris. He subsequently earned a Master's degree in Intelligence and International Security, with a major in Cybersecurity and Political Developments in the Middle East post-1945, from the War Studies Department of King's College in London. Following a number of positions in the private sector in Germany and abroad, Alexander worked as a research assistant for a member of the State Parliament of North Rhine-Westphalia, where he provided research and advice on digital politics and domestic security policy before joining BIGS.

IMPRINT

Located in Potsdam, the Brandenburg Institute for Society and Security is an independent, non-partisan, non-profit organization with an inter- and multidisciplinary approach with a mission to close the gap between academia and practice in civil security. The views expressed in this publication are those of the author(s) alone. They do not necessarily reflect the views of the Brandenburg Institute for Society and Security (BIGS).

Authors: Esther Kern, Alexander Szanto

Title: Cyber Supply Chain Attacks

Editor: Brandenburgisches Institut für Gesellschaft und Sicherheit gGmbH
(Brandenburg Institute for Society and Security)

Dr. Tim H. Stuchtey
(responsible according to the German press law)

BIGS Policy Paper No. 10, August 2022

Frontcover: Fritz Jorgensen/iStock Getty Images

ISSN: 2194-2412

Brandenburg Institute for Society and Security
Executive Director: Dr. Tim H. Stuchtey
Dianastraße 46 . 14482 Potsdam
Tel.: +49-331-704406-0 . Fax: +49-331-704406-19
E-Mail: info@bigs-potsdam.org . www.bigs-potsdam.org

BIGS
BRANDENBURGISCHES INSTITUT für GESELLSCHAFT und SICHERHEIT