

Cambridge Centre for Risk Studies

BitSight Technologies

CYBER SECURITY COST EFFECTIVENESS FOR BUSINESS RISK REDUCTION

Centre for
Risk Studies



UNIVERSITY OF
CAMBRIDGE
Judge Business School

BITSIGHT

Cambridge Centre for Risk Studies
University of Cambridge Judge Business School
Trumpington Street
Cambridge, CB2 1AG
United Kingdom
enquiries.risk@jbs.cam.ac.uk
<http://www.risk.jbs.cam.ac.uk>

Report Reference: Daffron, J., Copic, J., La Malfa, G., Jung, J., Sridhar, K., Ilardo, M., Coburn, A., Evan, T.; *Cyber Security Cost Effectiveness for Business Risk Reduction*; 2022; Cambridge Risk Framework series; Centre for Risk Studies; University of Cambridge.

Copyright © 2022 by Cambridge Centre for Risk Studies. All Rights Reserved.

Disclaimer Information: The views contained in this report are entirely those of the research team of the Cambridge Centre for Risk Studies, and do not imply any endorsement of these views by the organisations supporting the research, or our consultants and collaborators. The results of the research presented in this report are for information purposes only. This report is not intended to provide a sufficient basis on which to make an investment decision. The Centre is not liable for any loss or damage arising from its use. Any commercial use will require a license agreement with the Cambridge Centre for Risk Studies.

Cyber Security Cost Effectiveness for Business Risk Reduction

Contents

1	Executive Summary.....	4
2	Current State of the Cyber Threat.....	6
3	Digital Twins for Case Study Companies.....	14
4	Cybersecurity Controls.....	17
5	Ransomware Scenario.....	22
6	Data Breach Scenario.....	28
7	Cloud Outage Scenario.....	36
8	Summary of Results and Conclusions.....	43
9	References.....	46
10	Appendix	51

Cyber Security Cost Effectiveness for Business Risk Reduction

1 Executive Summary

In the world of cyber risk, there are three main categories of business data impact: confidentiality, integrity, and availability. In this report, we will look at two hypothetical attacks which predominantly affect data availability: ransomware and cloud outage, and a third attack which affects data confidentiality: data breach.

The following report details the current state of the cyber threat landscape in greater detail, as well as the process of modelling and parameterising a framework allowing corporates to quantify impacts from three cyber scenarios focusing on these three major trends. The framework is then applied to three case study companies in different sectors: Transportation, Apparel Retail, and Manufacturing. The primary result is the earnings value at risk over the next 5 years (5 yr EV@Risk) and the ratio of the scenario EV@Risk versus the baseline earnings value (EV).

EV@Risk Results

Losses from the three cyber scenarios modelled are expressed as the earnings value at risk for each of the three case study corporates, signified by the metric 'EV@Risk.'

The loss amount modelled in the L4 level can be as high as \$2.9 billion for Ransomware, \$1.9 billion for Data Breach and \$1.2 billion for Cloud Outage. Scenario losses range from 8 to 18 percent of EV for the Ransomware scenario, from 1 to 16 percent of EV for the Data Breach scenario and from 2 to 5 percent

for the most extreme level (L4) modelled. Taking the probability of an event occurring within the next five years into account, we get an expected EV@Risk. Summing the scenario expected EV@Risk for each case study company provides a total risk exposure metric. The total risk exposure for the Transportation company is \$140.07 million (or 2.25% of EV), for the Apparel Retail company is \$392.10 million (or 1.02% of EV) and for the Manufacturing company is \$148.89 billion (or 0.63% of EV).

Looking at the expected EV@Risk, the Manufacturing company is most impacted (% loss) by the Ransomware scenario driven by the direct impact to their production processes from the malware with a gradual return to full capacity. While for Transportation and Apparel Retail companies Data Breach is the most impactful (% loss) scenario. The Transportation company sees the biggest loss percent for the Data Breach and Cloud Outage Scenarios, with Manufacturing experiencing the largest percent loss for the Ransomware event.

When comparing the total risk exposure results in comparison to the BitSight ratings, the Manufacturing Company should be performing the worst overall, but its revenue dependency on cloud services and the amount of sensitive consumer data held are both much lower in comparison to the other companies represented. The losses faced by the Transportation company are in line with the low BitSight rating. The Apparel Retail company suffers the smallest exposure matching their high BitSight Rating.

Table 1: Summary of EV@Risk by Level by Scenario (Source: CCRS Analysis).

Case Study Company	Ransomware	Data Breach	Cloud Outage
EV@Risk, \$ millions			
Transportation	\$7.24 to \$1,162.66	\$25.8 to \$998.1	\$3.14 to \$199.18
Apparel Retail	\$22.95 to \$2,969.71	\$73.6 to \$1,979.6	\$44.44 to \$885.23
Manufacturing	\$27.26 to \$2,532.25	\$18.96 to \$227.38	\$4.82 to \$1,265.97
EV@Risk, % Loss			
Transportation	0.12% to 18.70%	0.41% to 16.05%	0.05% to 3.2%
Apparel Retail	0.06% to 7.73%	0.31% to 8.34%	0.12% to 2.30%
Manufacturing	0.11% to 10.67%	0.08% to 0.96%	0.02% to 5.34%

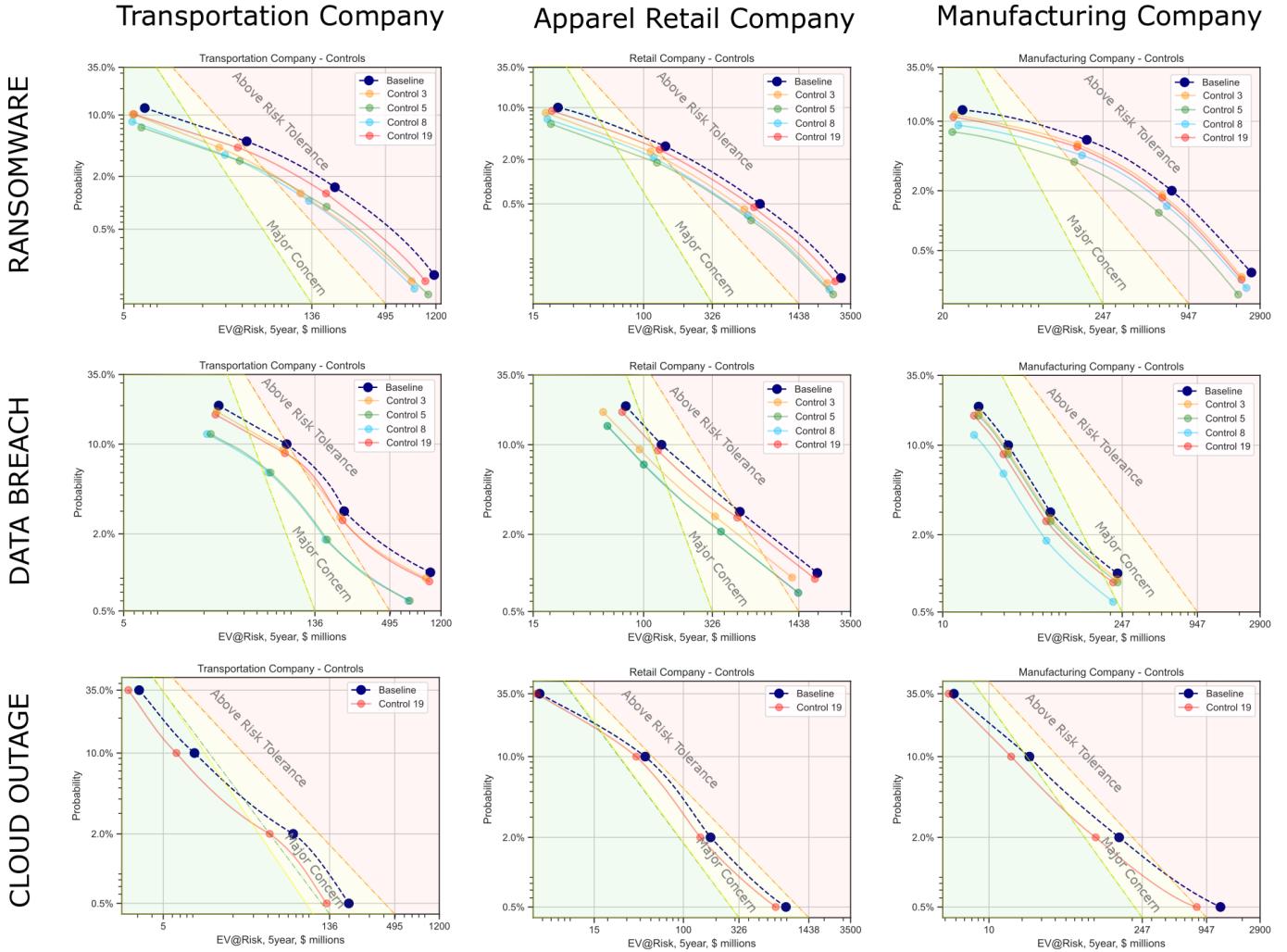


Figure 1: Risk Reduction by Scenario, Case Study Company, and Control.

Risk Reduction Results

This framework is expanded to quantify the potential risk reduction from implementation of control improvements. Four controls from the CIS Top 20 were selected for modelling:

- Control 3: Continuous Vulnerability Management,
- Control 5: Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers,
- Control 8: Malware Defences, and
- Control 19: Incident Response and Management.

The process of modelling these cyber security controls led to some interesting insights. The range of average risk reduction is 7% to 35% across all controls, case study companies and scenarios modelled. The results summaries per case study company, scenario, and control in Figure 1.

The Transportation Company sees the largest risk reduction by improving their malware defences (Control 8) for both the Ransomware and Data

Breach Scenarios. While for the Apparel Retail Company the configuration management (Control 5) gives the biggest return for Ransomware, and we see a tie between malware defences and configuration management in terms of returns for the Data Breach Scenario. Finally, the Manufacturing Company sees the greatest gain from Control 5 for the Ransomware scenario and Control 8 for the Data Breach scenario. For Cloud Outage, only one control was modelled, yet it is insightful to see potential gains for just improving the company's incident response plan (Control 19).

Organisations can use this framework to better examine the risk-reward trade-offs of implementing specific controls solutions. Further, this approach and the results in this report could be used to determine return on investment (ROI) from specific control improvements and contingency plans.

2 Current State of the Cyber Threat

In the following section, we will first discuss the main trends related to the infiltration of a computer system. We will respectively cover the case of a ransomware attack and a data breach attack. We then complete the picture with an analysis of cloud outage.

Ransomware attacks aim to ‘infect’ the company, holding its data and systems “at ransom,” making users unable to access the firm’s systems. A ransom sum, often in a cryptocurrency, is demanded, after which the hacker may grant the company access to its systems once again. Data breaches aim to attack a company system in order to take possession of data. In some cases, a ransom is demanded in exchange for the ‘return’ of the data or a promise not to publish them. It is the responsibility of a company to protect sensitive data including payment and health records. In the event these types of data have been comprised, companies are required to pay punitive fines and offer compensation.

Cloud outage refers to the temporary unavailability of the cloud infrastructure. Worldwide cloud infrastructure an integral part of the operational activity of around 50% of all companies.¹ Average enterprise cloud adoption in Europe is 36% and peaks at 70-75%.² Without an in-house server or system, companies will suffer expensive down time during the loss of the cloud computing and storage capacity.

Current State of Cyber Risk

The main trends related to cyber risk change yearly due to market conditions (both on the side of the actors and on the side of the victims), economic and social framework and technological advancement.

In 2020 and 2021, the biggest event that shocked the market was the Covid-19 pandemic. The pandemic had an immense impact on the cyber risk landscape, leading to an evolution of cyber risk attacks. The transition to working from home has forced a change in the way the vast majorities do business and maintain relationships both within and without their own networks. This has opened a host of new vulnerabilities and pushed a rethink as to how to apply suitable and company-wide protections against the threat of cyber attack. Forms of risk mitigation have also changed: in addition to new forms of technological protection, new backup methods, new risk reporting procedures and staff training have been rolled out.

¹ (Statista 2021)

² (Eurostat 2021)

Cyber actors took advantage of the resettlement situation and quickly diversified the forms of attack. New and changeable working conditions generally only broadened the gaps in cyber protection, at least in the early months of the pandemic with those companies which were already vulnerable to attack, proving to be the worst affected in this period.

For example, phishing has always been a popular strategy among cyber actors seeking to gain entrance to secured systems, but methods evolved substantially through the pandemic as attackers began to prey on pandemic paranoia to lure in vulnerable users. Phishing commonly refers to the attempt to trick a victim into clicking on a link or opening an attachment in an e-mail (e-mail phishing). However, in addition to e-mail phishing, there are four other categories of phishing:

- *Vishing*: the attempt to extort information through a call and the simulation of a support call centre.
- *Smishing*: the attempt to extort information through a text message.
- *Spear phishing*: the same as that of e-mail phishing, but the techniques used to attract the attention of victims and induce them to click are much more sophisticated and often rely on psychological feelings such as fear and the need to do something quickly.
- *Whaling*: the focus on targeting specific C-suite employees.

Experts agree that phishing practices are on the rise and remain an extremely effective weapon for both gaining access to, as well as pressuring, businesses. This second aspect is often under considered but is actually a highly effective social engineering tool for hackers in many cases. The reduced sense of security in companies due to the pandemic and a general lack of clarity in decision-making has triggered the proliferation of phishing techniques to create panic; this greater insecurity means a greater likelihood of successful ransom payments.

Related to this point is the increase in doxing practices throughout the pandemic. Doxing refers to the publishing of private data that is extorted from companies through attacks, typically names, homes addresses, and salaries. When resistance to an attack

is encountered, hackers may use doxing to push their agenda, demonstrating their capabilities and willingness to leak data and putting more pressure on victims. All this increases the likelihood of a successful ransom pay out from an attack.

Additional pressure attacks concern data backups. Evidence shows that hackers have the possibility to access and encrypt backups as well. An even more aggressive practice is to threaten to delete backups - weaponising the panic and paranoia is a key component of the negotiation phase for cyber actors.

Ransomware Trends

The impact of ransomware in cyber risk has grown dramatically in the last two years (2020-2021) with an escalation due to the pandemic. Until 2019, data exfiltration was the biggest driver for cyber insurance demand (more than 50% in cyber risk). Since 2020, the trends have changed, and ransomware has become the item attracting the most insurance cover (from 13% in 2019 to 54% in 2020).³ The data shows that hackers are more active than in the past to make corporate systems inaccessible now that the pandemic has forced the reorganisation of remote working and extended the attack surface.

Trends indicate that ransomware attacks are now increasingly targeting single corporate networks, rather than trying to hit a spread of machines across a myriad of different systems. We believe there is greater leverage in both extorting larger companies and negotiating larger payments. From 2019 to 2020, the average ransom demand amount doubled due to this change in targeting. The effect of the pandemic on big business has undoubtedly undermined the certainty of being able to defend against attacks, given the unpredictable vulnerabilities brought about by new and flexible working conditions.

As with data breach, negotiation has become an important aspect of ransomware campaigns. Once the attack has taken place, the victim has a short time to respond to demands. During this period, negotiation takes place: the hackers propose a ransom and the victim, if they decide to pay, attempts to discuss. As several events have shown, the threat of doxing (also called multi-faceted extortion events) has guaranteed a higher probability of ransom payment. This is because the technical capabilities of ransomware groups now include data exfiltration techniques which add to the extortion potential of the attack due to the added costs and reputational damage a business would face in the event of non-payment are higher.

³ (BitSight Technologies 2021b)

There is a wide range of reasons victim organisations might be pushed to pay a ransom, including:

- Technical challenges with backups
- Attacks may target the board of directors to have a greater impact on the decision-making processes of companies
- Reputational damage
- Timing and doxing pressure from the hackers
- Estimated impact of the attack
- Inability to estimate the damage without system access

Cyber insurance will cover the payment losses

The sectors most affected by ransomware are those with the most fragile systems, including education, manufacturing, and healthcare. The education and manufacturing sectors have historically been weak due to the low levels of protection.⁴ A high profile ransomware and data breach attack on Colonial Pipeline caused a six-day disruption to the north-eastern US, resulting in gas shortages. Impact was limited, however, due to the company paying DarkSide, the hacking group responsible for the attack, \$4.4 million in ransom. Research by BitSight shows that “62% of the largest U.S. Oil and Energy companies are at heightened risk of ransomware attack.”⁵ The healthcare sector has been a profitable target given the great strain it has experienced throughout the pandemic, with no resiliency in hospital networks to allow even time for negotiation in most ransomware attacks. Another sector that has historically been at risk is the IT sector as it represents a hub for access to many companies (third-party liability).

Data Breach Trends

The number of stolen data has risen sharply in the pandemic period as new vulnerabilities in computer systems have emerged. Some reports refer to a doubling in the amount of data that was exfiltrated in 2020 compared to 2019.⁶ Data breach attacks focus on profitable, vulnerable sectors, such as healthcare, IT, finance, and manufacturing.

Statistics show that the main causes of data breaches are hacking, errors, malware, and physical attacks. Usually the hackers are external actors, often part of real criminal organisations, though it is not uncommon for internal actors and/or members of staff to be involved or entirely responsible.

⁴ (Hiscox 2021)

⁵ (Olcott 2021)

⁶ (RiskBased Security 2021)

In recent years, high ransom demands from hackers that have been matched by actual payments from customers have increased the value to risk of data breaches. The largest part of the data breach losses is associated with compensations companies must pay to affected users, as well as the damage to firm reputations. Costs are related to the size of the data breach but also to the type of data exfiltrated which can be categorised a number of ways: PII (Personally Identifying Information), PHI (Protected Health Information) and PCI (Payment Card Industry). PII is the least sensitive data and concerns people's personal details as well as some data linked to their profession. PHI is extremely sensitive as it is considered highly protected and private data concerning confidential health details. PCI is potentially the most disruptive data when stolen because it concerns financial credentials and can trigger a chain of extortion. While PHI and PCI data is highly desirable, it makes up the minority of data exfiltrated in all breach attacks. This is due to the different security layers in place to protect the most sensitive data.

Cloud Outage Trends

As the cloud is a shared service, an outage usually affects multiple companies at the same time. On an economic level, a cloud outage could disrupt an entire industry across one or more regions. An emblematic example of a business disruption chain is the recent case of Google.⁷ On 16 November 2021 at 9:34 am (US/Pacific), Google's cloud platform suffered a global outage due to a bug in the network configuration, bringing down many services including Spotify and Facebook. The malfunction lasted about two hours. The technical problem seems to be linked to Google's "Cloud Load Balancing" service, which allows the distribution of computational resources over one or more regions according to the customer's needs. For large companies, an outage of just a few hours can have a major price tag because of its cascading impact. A malfunction can trigger a chain of disruptions on a large scale, leading to huge economic losses.

Cloud failure caused by an external attack is an ever-evolving risk. The first vulnerability that would permit an outside influence to run code in the environments of other users was recently discovered and named Azurescape⁸ (due to its discovery on Microsoft Azure platforms). The code enables privilege escalation out of container environments (over an entire cluster of containers) opening to hacker actions like sabotage or execution of malicious code. This type of vulnerability opens up a range of unprecedented scenarios both in

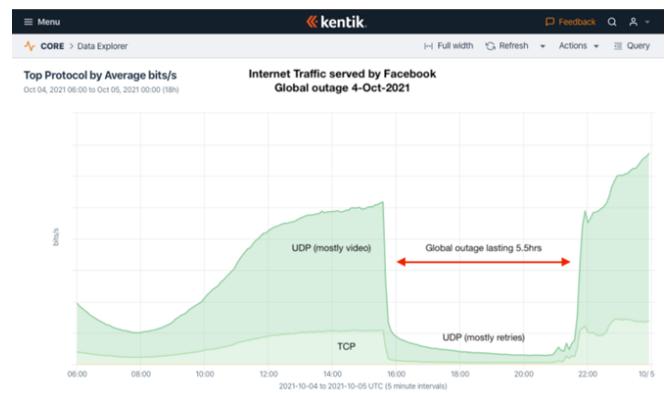
terms of type and scale of risk. Potentially, this type of cloud (CaaS: Container-as-a-Service) offers the sharing of a service managed in separate environments to a large audience. Despite the big investments made by providers to ensure security, it is not impossible to imagine that an attacker could breach privileges and enter other users' environments. The possible chain of risks that would be triggered could represent an unprecedented scenario for the cloud.

On 4 October, Facebook underwent an outage lasting about six hours that affected most of its applications/subsidiaries (Messenger, Instagram, WhatsApp). Facebook reported on the cause of the outage:

"Our engineering teams have learned that configuration changes on the backbone routers that coordinate network traffic between our data centers caused issues that interrupted this communication. This disruption to network traffic had a cascading effect on the way our data centers communicate, bringing our services to a halt".⁹

This event demonstrates that a significant cloud outage may come from internal system errors or misconfigurations. As reported by analysts, these types of misconfigurations have enormous technical consequences that spill over into the inability of users to access services.¹⁰

Figure 2: Facebook's Outage Analysis (Source: Kentik Data Explorer).¹¹



When analysing the historical events that have caused cloud outages for major providers, many of them can be traced back to misconfigurations, software bugs and resource exhaustion. There is no explicit evidence of attacks on cloud systems that have led to outages at this time. However, the publications made by the

⁷ (Google 2021)

⁸ (Zelivansky and Avrahami 2021)

⁹ (Janardhan 2021)

¹⁰ (Madory 2021)

¹¹ (Kentik 2021)

providers themselves are difficult to decipher and malicious actors may or may not have played a role in some outages. This potentiality represents the point of contact between the three scenarios in this report (Ransomware, Data Breach and Cloud Outage).

Cyber Threat Actors

Cyber Threat Actors are agents in actions or processes that are hostile or intend to cause harm through cyber means. Such actors can be classified into one of five different groups based on their motivations and affiliations and are typically associated with different Tactics, Techniques, and Procedures (TTPs). The focus of current attacks is on Confidentiality and Availability, but Integrity would be the most impactful attack for organisations and therefore should be explored as a hypothetical.¹²

Cyber criminals are mostly profit-driven and account for most cyber events. They primarily target organisations' data to sell, hold for ransom, or otherwise exploit for monetary gain. Cybercriminals may work individually or in groups to achieve their purposes and often operate out of countries where governments are either unable or unwilling to prosecute their activity – if somewhat aligned with their strategic goals. More and more criminals are joining the game as there are new black-market services available for novices. In fact, although financially-motivated, cybercriminal operations may be very impactful for society at large when targeting, directly or indirectly, critical infrastructure that is essential for the functioning of an entire country-system including power grids, transport networks, information and communication systems, pipelines, water treatment plants, manufacturing facilities, and similar. Their most common TTPs include phishing, social engineering, business email compromise, scams, botnets, password attacks, exploit kits, malware, and ransomware.

Nation state actors aggressively target and gain persistent access to public and private sector networks to compromise, steal, change, or destroy information. The main driver behind nation state actor's cyber activity is, by far, espionage. These groups are most typically part of a state apparatus or otherwise state-proxies receiving direction, funding, technical assistance, or political protection from a nation-state. Nation-state are usually associated with Advanced Persistent Threat (APT) – although the latter refers to a type of activity that can be conducted by a range of actor types, not only states. The motives behind nation-states' cyber operations range from gaining political and economic advantage

over competitors and/or adversaries on the global stage to support military operations. Their most common TTPs include spear-phishing, password attacks, social engineering, direct compromise, data exfiltration, remote access trojans, and destructive malware. While they do not account for the majority of cyber events, nation state attacks are concerning due to their potential scale and economic impact.

Cyber terrorists are politically motivated non-state actors with limited offensive cyber activity that is typically disruptive in nature or otherwise dedicated to propaganda and recruitment efforts. In fact, terrorist organisations primarily use their cyber skills to safely communicate and recruit on encrypted channels and their most common TTPs are defacements and claimed leaks. The technical as well as organisational resources needed to cause physical destruction through cyber means seem to be still out of reach for militant extremists, yet a growing tendency for such groups to advocate the use of cyber on their networks suggests that there is no lack of intention to develop them in the near future. Moreover, recent analysis shows a growing sophistication in terrorist groups' cyber operations, which now include cyber espionage and theft.

Hacktivists are politically, socially, or ideologically motivated non-state criminal hackers who target victims for publicity or to induce change in the pursuit of their strategic goals. Their activity is most commonly limited in both scope and sophistication but can sometimes result in high profile operations. They are usually non-governmental individuals that can be affiliated to both licit and illicit organisations. Their most common TTPs are DDoS attacks, doxing, and website defacements. However, recent activity – including the compromise of states' surveillance systems and broadcasting platforms as most recently displayed in Belarus and Iran – shows a growing depth and breadth of hacktivists' operations suggesting a new level of technical and strategic sophistication among groups.

Malicious insiders are current or former disgruntled employees, contractors, or other types of partners who have authorised access to an organisation's networks, systems, or data, and that intentionally exceed or misuse their access in a manner that negatively affects the confidentiality, integrity, or availability of the organisation's information or systems. Their primary motivation is usually financial gain or revenge, and their most common TTPs are data exfiltration or privilege misuse.

Nation-State activity

Recent research highlights how, in recent years,

¹² (Fruhlinger 2020)

nation-state cyber attacks have increased drastically in numbers, sophistication, and impact. For instance, a study conducted at the University of Surrey and sponsored by HP drawing upon intelligence gathered from informants across the dark web and input from a panel of 50 leading practitioners in relevant fields, points out that attacks are becoming more frequent, varied, and open, moving us closer to a point of ‘advanced cyberconflict’ than at any time since the inception of the internet. Findings show a 100% rise in ‘significant’ nation state incidents between 2017-2020, with the favourite targets being the private sector (35%), cyber defence (25%), media and communications (14%), government bodies and regulators (12%), and critical infrastructure (10%).

Based on incidents recorded during the past twelve months, we observed nation states increasingly devoting significant time and resources to achieving strategic cyber advantage to advance their strategic interests, intelligence gathering capabilities, and military strength through espionage, disruption, and theft. In its 2021 Annual Threat Assessment, the US Office of the Director of National Intelligence (ODNI) warned that, “cyber threats from nation states and their surrogates remain acute. Foreign states use cyber operations to steal information, influence populations, and damage industry, including physical and digital critical infrastructure.” Our analysis shows that China, Russia, North Korea, and Iran remain the most active nation-states in the cyberspace, both directly with APTs linked to their government/intelligence services, and indirectly with non-state-actors operating within their borders and broadly in support of their policy objectives.

Cyber espionage remained the most persistent threat – further enhanced by worrisome trends such as supply chain attacks – as recent incidents and attempted attacks demonstrate. Last December, emblematic was the example of the SolarWinds Orion cyber breach attributed to hackers tied to Russia’s Foreign Intelligence Service and that targeted government agencies and private sector organisations all around the world. On the other hand, destructive cyber attacks – those that have as their main goal the physical destruction or damage of their target – are still a rare occurrence. The few instances of such attacks recorded in recent times have very rarely resulted in physical damage and have rather been limited to data destruction through deletion or encryption without the possibility of recovery. This has been the case for the few certified attacks of this kind disclosed over past year, all concerning threat actors operating out of Iran and Israel deploying data-wiping malware to destroy their targets’ networks and disrupt each other’s infrastructure.

Finally, disruptive cyber attacks resulting in disconnections and disruption of access to and operation of multiple or vital digital systems and services, although rare, occur more often than destructive attacks and, just like the latter, have more chance to take place in proximity to conflict-affected areas or in contexts characterised by high geopolitical tensions. Incidents recorded in the past twelve months occurred saw China targeting India’s transport sector and Russia targeting Ukraine’s security and defence networks, right as tensions started to escalate at the border for both countries and their respective neighbours.

Figure 3: Nation state incidents in 2021 by Country
(Source: CCRS Analysis)

Nation-state incidents in 2021* - by country

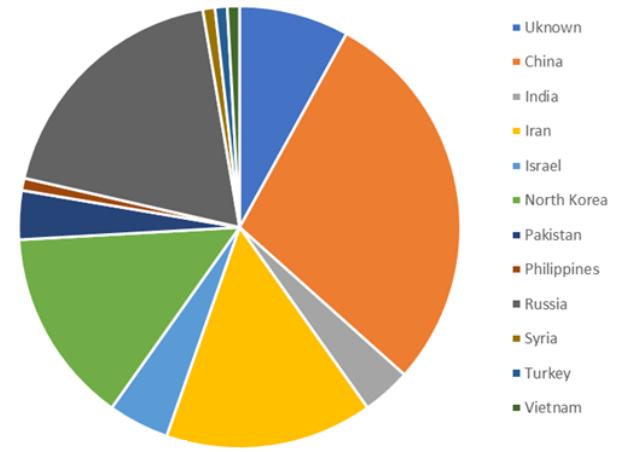
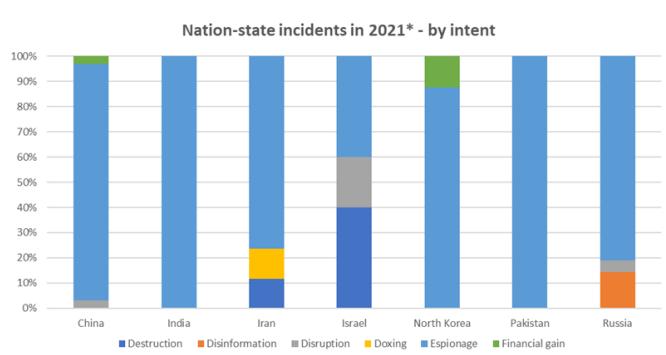


Figure 4: Nation-State Incidents in 2021 by Intent
(Source: CCRS Analysis).



Digital Supply Chain Risk

In the fall of 2019, SVR, a Russian intelligence agency, breached the corporate network of SolarWinds, a software company, and implanted malicious code, called Solorigate, into the update its popular Orion

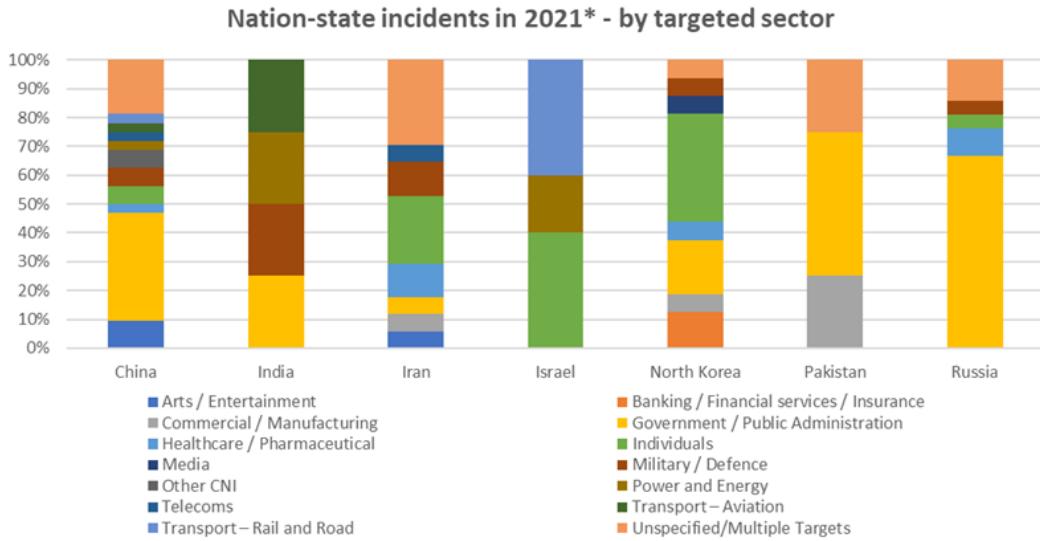


Figure 5: Nation-State Incidents in 2021 by Target Sector (Source: CCRS Analysis).

cloud management tool. This furnished SVR with an attack vector into the 18,000 customers that installed the update.

Solorigate enabled SVR to enter into the networks of SolarWinds customers. To evade detection, SVR did not aim to enter into every network but picked the most strategic targets. Once inside, SVR exfiltrated sensitive data and in some cases, passwords, and decryption keys to enter other networks. They also gained access to “red-team tools”—attack methods that cybersecurity companies use to test the defences of their clients—which they could employ to infiltrate future targets. The attack was only publicly discovered in December 2020 by FireEye, a cybersecurity company which had also been breached by Solorigate.

While SolarWinds was the first attack vector that the information security community identified, it was not the only supply chain component that was compromised. In total, nine US government agencies and 100 private companies were breached. While the attack was an intelligence operation and SVR did not damage any technology systems, it will take years for US government organisations to be confident that Russian intelligence is no longer present within their networks.

In the wake of the SolarWinds attack, technologist Bruce Schneier noted that the company and its private equity investors skimped on security to increase profit margins. It outsourced most of its software engineering, hiring cheap coding labour overseas. It had poor security practices; just a few years ago, it set a critical server password to be “solarwinds123”, and it had failed to stop—or even detect—numerous cyber incursions in the past....

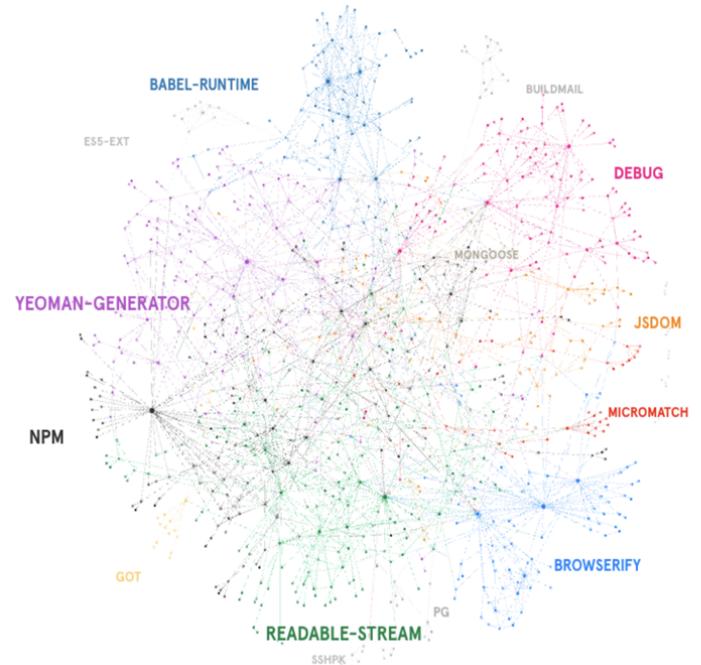


Figure 6: The complexity of digital supply chains (Source: (Arikan 2017)).

Figure 6 shows a “dependency graph” of the 100 most downloaded JavaScript packages that were published through a popular package manager (called NPM Registry) and the four levels of package dependencies; it illustrates the complexity of software supply chains.¹³

Both supply chain components produced by vendors and drawn from open-source libraries are vulnerable to infiltration.

Software vendors regularly incur technical debt; they make decisions which are expedient in the short-

¹³ (Arikan 2017)

run, enabling them to more quickly and cheaply deploy their products, but which can increase costs in the long-run.¹⁴ For instance, many software companies release products without suitably testing them for security flaws. A study by Diffblue, a UK cybersecurity company, found that developers spend 35% of their working hours testing their products, but most of this time is spent ensuring functionality, not cybersecurity.¹⁵ The cost of this technical debt is then passed on to the end customer; when a cybersecurity vulnerability is exploited, it is the software user—and the software user's customers—who suffer.

Open -source libraries, like those available for JavaScript, Java, python, R, Ruby and so on, are similarly vulnerable. These libraries are not produced by trusted foundries, rather, the source code is freely available and developers are given free rein to modify and update libraries. Some of these developers have scant quality control processes and write error-ridden code. Worse yet, criminal groups can perpetrate “trojan horse attacks,” whereby they lodge malicious code into open-source packages. Finally, open-source software products lack dedicated security teams who can develop and distribute patches to affected users once vulnerabilities are discovered. For all these reasons, open-source libraries are highly insecure.

There are still more supply chain threats facing businesses. To reduce costs, small and medium enterprises (SMEs) often outsource IT management to contractors. These contractors, called managed service providers (MSPs), use software to remotely monitor and run corporate networks. As one former NSA official has noted, if an adversary successfully attacks these systems, they are “in god mode.”¹⁶ With administrative control over technology accounts, they can exfiltrate sensitive data or permanently shut down critical technology systems.

A number of major companies and government agencies across industries and around the world have been greatly affected by supply chain vulnerabilities and attacks.

Such attacks are only becoming more frequent. Paul Nakasone, the Commander of US Cyber Command, has said that cyber attackers are perpetrating supply chain attacks at “a scope, a scale, [and] a level of sophistication that we hadn’t seen previously.”¹⁷ The security firm Sonatype has estimated that there was over 400% more supply chain attacks between July 2019 and March 2020 than in the previous four years combined.¹⁸

Moreover, the global economy has yet to experience the full supply chain attacks at their full potency. The SolarWinds campaign was an intelligence operation the Russians team responsible did not subvert norms or attempt to damage or disrupt the government agencies they compromised. Other infections have been hindered in their impact by the sophistication of their malware, the motivations of their actors, or the countermeasures, either purposeful or accidental, the attacks were met with. In the future, companies may not be so lucky. The vulnerability and exposure of global software supply chains must form a central pillar in cyber security discussions for all companies dependent even in small part on outside services for the carriage of daily business.

Cyber Events Regulatory Reporting

In February of 2018, the Securities and Exchange Commission (SEC) issued guidance reminding companies that are publicly traded on US Exchanges that they must disclose “material” cyber incidents to investors and the general public. It stated that companies must reveal that they were victims of an attack if “there is a substantial likelihood that a reasonable investor would consider [this] information important in making an investment decision.”¹⁹ The regulators stated that many cyber attacks would be important to “reasonable investors” because the US economy and capital markets “depend on the security and reliability of information and communications technology, systems, and networks.”²⁰

The Electronic Data Gathering, Analysis, and Retrieval (EDGAR) database, which collects and stores all documents that publicly traded companies submit to the SEC.²¹ This database enables an analysis to see what cyber attacks companies have reported in the three-and-a-half years since the SEC issued its cyber directive. The focus was on 8-K and 6-K reports, which US-based companies, and their foreign counterparts, are required to file whenever there is a material development—such as a large new order, a supply chain breakdown, or a cyber attack. A set of cyber related key words was used to search these documents.²² Then a manual validation was completed to confirm these companies were actually reporting a cyber attack in these fillings. In total, there are 87 companies reporting a cyber incident in the approximately three-and-a-half years between 21 February 2018 and 1 September 2021.

Clearly, more companies than this are concerned

¹⁹ (Clayton 2018; SEC.gov 2018a; 2018b; SEC 2018)

²⁰ (Clayton 2018; SEC.gov 2018a; 2018b; SEC 2018)

²¹ (SEC.gov 2021c)

²² Keywords used: “cyberattack,” “cyber attack”, and “cyber-attack”; “hack,” “hacker” and “hacked”; “ransomware” and “malware”; and “data breach,” “data loss” and “data leak”.

about the threat of about malicious cyber attacks. Thousands of companies warn that they may miss revenue projections if they suffer from a cyber attack; cyber events are included as *force majeure* provisions in service agreements and contracts; and, before completing a merger, purchasing companies require certification that their acquisitions' technology assets have not been infiltrated or compromised.

Most companies, however, maintain that they have not been affected by a material cyber event. For example, one company states that while it has "experience[d] cybersecurity [sic] attacks of varying types and degrees on a regular basis...to date, none of the incursions identified have had a material adverse effect on our business."²³ But while an event may not cause a materially adverse effect, it may still be materially important to a company's outlook. History of a cyber attack may indicate inadequate security measures, so companies that are compromised may be vulnerable to a materially adverse incursion in the future. This is clearly something a reasonable investor would care about.

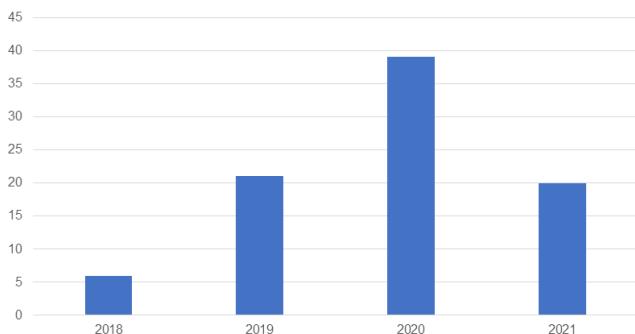


Figure 7: Material Cyber Even Reporting Trend of 8-K and 6-K Fillings (Source: CCRS Analysis).

Even so, it appears that the SEC is reluctant to exercise its regulatory authority, except in the most egregious cases. In its two most prominent actions, the SEC fined education technology company Pearson for failing to file an 8-K about a data breach involving thousands of student records and settled charges against insurer First American for covering up vulnerabilities that "exposed over 800 million title and escrow documents."²⁴ Lesser offenses have escaped regulatory scrutiny. Consequently, investors are largely in the dark about the cybersecurity postures of thousands of publicly traded companies.

Interesting insights, however, can be gleaned from those cyber incidents that companies choose to report, see Figure 7. In 2020, there were 85% more reports than in 2019—a problem likely exacerbated by the

COVID-19 pandemic, which accelerated the digital transformation and increased the potency of cyber attacks. In 2021, the volume of reports is lower; 2021 is on pace for 30 reports from companies, a decrease of 30%. Perhaps firms have hardened their defences as work-from-home has become the norm.

Over 90% of the reports described the tactics—ransomware, supply chain attack, data breach, malware, encryption, distributed denial of service—that the attackers employed, see Figure 8. Fifty-six percent of the reported incidents were ransomware attacks, while only six percent of incidents were supply chain attacks. But these figures are likely distorted. Ransomware attacks are noisy. Attackers encrypt files and computer systems and quickly inform the victims in order to earn a ransom. By contrast, many supply chain attacks are perpetrated by more sophisticated nation-states, who want to gain intelligence and steal IP. As a result, they cover their tracks to evade detection. Many companies are likely unaware that they have fallen victim to a supply chain attack.

Finally, 10% of the incidents were not targeted against companies, but their contractors. Aviat Networks, for instance, reported that "its fiscal 2020 second quarter and first half results are anticipated to come in lower than previously forecasted due to a cyberattack at one of the Company's contract manufacturing vendors. This effectively shut down the vendor's production and shipments of Aviat products for a three-week period."²⁵ This suggests that companies don't have to worry only about their own cybersecurity; they also have to worry about the cybersecurity of the companies that they depend on and must evaluate the cybersecurity practices of their potential vendors and partners to avoid such shocks.

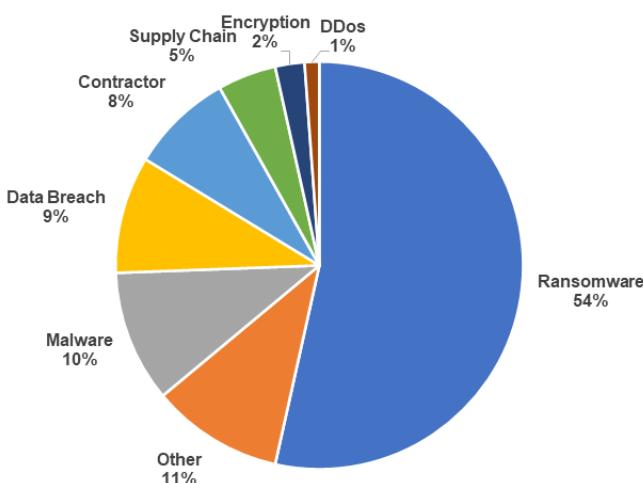


Figure 8: Type of material cyber reported in 8-K and 6-K Fillings (Source: CCRS Analysis).

²³ (SAP 2020)

²⁴ (LaCroix 2021b; 2021a; SEC.gov 2021a; 2021b)

²⁵ (Aviat Networks 2020)

3 Digital Twins for Case Study Companies

Financial Digital Twins

To measure the fiscal impacts of the pressing trends in the cyber threat landscape, we have developed three scenarios (i.e., ransomware, data breach and cloud outage), and selected three case study companies in different industry sectors to model the effects of the shock. It is also notable that the case study companies have different product portfolios, business models and operations. However, all case study companies share a few key similarities: they all have high raw material costs and complex supply/distribution channels, which require a high level of efficiency and precision in managing the resource allocation processes indicating heavy reliance on IT capabilities.

The details and general characteristics of the case study company are provided in Table 2 below. We consider a publicly traded companies belonging to three different sectors: Transportation, Apparel Retail and Manufacturing. We gathered real cash flow data for each of these companies and then anonymised each company in an effort to keep the focus on the modelled results for these three generic companies than the focus on findings for the three specific companies.

We have developed “digital twins” of these case study companies – discounted cash flow models designed to represent the case study companies’ exposure to impacts caused by financial, markets and geographic externalities in a simplified but standardised manner. This is a preparatory step to establish a baseline for our scenarios, which will help us to specify scenario drivers based on the narratives we developed. We model a five-year projection starting in 2021.

The result of our projections produced five-year earnings value (5-year EV), a sum of case study firms’ projected free cash flow figures discounted with the weighted average cost of capital (WACC) derived from market references. We use five-year earnings values for the case study companies to establish the baselines for our scenarios, against which the impact of the scenarios will be measured, producing a metric: five-year Earnings Value at Risk (5-year EV@Risk). There are items included under revenue and cost categories of the projections such as raw material costs, labour costs and capital expenditures. Along with market breakdowns these items are used to determine our case study companies’ organisational profiles and geographic sensitivities to the scenario shocks we specify.

Table 2: Three Case Study Company Summary Attributes

Case Study Companies	Company 1 	Company 2 	Company 3 
Industry Sector NAICS	Transportation (48111)	Apparel Retail (4481)	Manufacturing (334511)
Head Office Location	Europe	Europe	US
Employee Count	10,000+	200,000+	500,000+
Markets	Europe, Asia & Africa	Global	Global
Products	Regional air passenger transportation service	Family clothing & accessories	Instruments and Related Products Manufacturing for Measuring, Displaying, and Controlling Industrial Process Variables
5y Earnings Value	US\$6.2bn	US\$38.4bn	US\$23.7bn
Industry/company Profiles	<ul style="list-style-type: none"> • High raw material costs • High net CapEx • No service in Americas 	<ul style="list-style-type: none"> • High raw material costs • Low depreciation & amortisation • Global supply chain 	<ul style="list-style-type: none"> • High raw material costs • Significant labour costs • Global distribution

Although the starting point for each of these case study companies was a real organisation, we have taken additional steps to anonymise the identity of the companies referenced; we have modified the revenue figures and size of market exposures, but % allocation to cost variables (i.e., the core sensitivity to scenario drivers) remain unchanged.

Location Breakdown

Business assumptions for the three companies are shown in Table 3. We assume that the Transportation company, considering the type of business, has a concentration of its activities in Europe. The retail company has a big share of its activities in Europe and other considerable shares in both Asia and Americas. The Manufacturing company on the other hand has activities based in the Americas and the rest divided between Europe and other countries.

Table 3: Location Breakdown by Case Study Company

Company/Sector	Business Location	Percentage of the Business
Transportation Company	Europe	96%
	Other	4%
Retail Company	Europe	63%
	Asia	19%
	Americas	17%
	Other	1%
Manufacturing Company	Americas	67%
	Europe	23%
	Other	10%

Table 4: Summary of Cash Flow Categories Impacted by Each Scenario

Cash Flow Category	Cash Flow Element	Ransomware	Data Breach	Cloud Outage
Revenue Shock	Revenue	X	X	X
Routine Costs Shock	Labour Costs	X		
	Marketing and PR	X	X	X
	Data Software and Maintenance	X	X	
Non-Routine Costs Shock	Impairment on PPE	X	X	
	Incident Response Costs	X	X	X
	Legal Settlements	X	X	X
	Regulatory Investigation and Fines	L4 only	X	
	Compensation Costs	L4 only	X	
	Ransom Payments	X		
	Other Costs		X	

Cash Flow Impacts by Scenario

To get to a 5-year EV@Risk we need to impact various elements from the cash flow. The table below shows the scenario variables in the cash flow model that construct the financial digital twins for our case study companies and the variables impacted by different scenarios. We model 4 levels of each scenario (called L1 to L4) with the intent that it explores the entire distribution of losses possible for the given scenario. In this regard, not all cash flow elements are impacted in each level. For the ransomware scenario we have added a data breach to the narrative for the L4 level and thus Regulatory Investigation and Fines and Compensation Costs are only impacted in the L4 level.

Cyber Digital Twins

The following table summarises some key cyber digital twin elements for each case study company based on BitSight's outside-in telemetry. The Apparel Retail company has the best overall BitSight rating, yet it is in a sector where 4.2% of its sector outperforms it. The Transportation company has a much lower rating and yet is performing well in their sector, while for the Manufacturing company it is the opposite, they have a low score and 8.7% of their sector is performing better than them. We also feature the botnet infections grade and the potentially exploited grade, these are scored on a scale from A to F, where A represents a minimal risk and F represents an increased risk. Research conducted by BitSight highlighted that "the data shows that organisations with a rating lower than 600 are 6.4x, and organisations with a rating between 600-650 are

4.6x more likely to be a ransomware victim compared to the benchmark of organisations with a 750+ rating".¹

In addition to these outside-in observations, it is helpful to have internal insights to aid in the loss modelling. The desired data points differ by scenario model. For ransomware we need to know the number, type, and revenue dependency of endpoints (i.e., desktops, laptops, cell phones, tablets, servers and/or sector specific-IT assets). For data breach, it is helpful to know the type and amount of data held in which geographies. Finally, for cloud outage it is useful to know that cloud architecture including the revenue dependency by cloud service.

¹ (Cadet 2021)

Table 5: Cyber Digital Twin Attributes by Case Study Company

Case Study Companies	Transportation 	Apparel Retail 	Manufacturing 
BitSight Rating ¹	640	790	620
Sector Mean	718	723	722
Sector Median	730	740	730
Sector Percentile for BitSight Rating ²	91.3%	99.5%	95.8%
Botnet Infections Grade	A	A	A
Potential Exploited Grade	A	A	A
Increase in Risk of Ransomware	4.6	1.0	4.6
Patching Cadence	B	A	C

¹ As of October 2021

² As of October 2021

4 Cybersecurity Controls

There is a wide range of cybersecurity mitigations or control taxonomies and standards available to corporates. Security controls can be viewed as descriptions of the safeguards and protection capabilities appropriate for achieving the particular security and privacy objectives of the organisation and reflecting the protection needs of organisational stakeholders.¹ We have reviewed seven different control taxonomies and security standards, logos provided in Figure 9.

Security Controls Taxonomy and Standards



Figure 9: Security Controls Taxonomy and Standards Reviewed

NIST Information Security and Privacy Controls (SP 800-53 Rev. 5) features 20 high level families, with 306 controls and over 715 control enhancements.² This controls taxonomy sits within the 'respond' step of NIST's Cybersecurity Framework. We found this to be a widely used reference control taxonomy. ISO/IEC 27001 Information security management has 14 high level controls with numerous sub controls.³ NIST addresses information flow control broadly in terms of approved authorisations for controlling access between source and destination objects, whereas ISO/IEC 27001 addresses information flow more narrowly as it applies to interconnected network domains. MITRE has developed a taxonomy of Tactics, Techniques and Procedures (TTPs) with 43

unique mitigations (called Enterprise Mitigations v8) connect to these TTPs with no high level group, but still a more trackable list of controls in comparison to the other standards already mentioned.⁴ The Centre for Internet Security has created a 20 CIS Controls v7.1 (called the Top 20) featuring 20 controls with 171 plus sub controls with measurement methods, sensors and metrics detailed.⁵ A sensor which helps monitor several of the controls is System Configuration Enforcement System.

We reviewed two industry standards on cyber security as they provided robust taxonomies for review. We first looked at SOC 2, which is global information security audit standard targeted at organisations that provide IT services and systems to clients (for example, Cloud computing, Software as a Service, Platform as a Service). It was developed by the American Institute of CPAs (AICPAs), meaning that it is very popular in the US and many major companies list that they are SOC 2 compliant.⁶ We also looked at the Cloud Security Alliance (CSA) CAIQ v3.1 which documents what security controls exist in IaaS, PaaS, and SaaS service, similar to the SOC 2.⁷ CAIQ is not intended to duplicate or replace existing industry security assessments but to contain questions unique or critical to the cloud computing model in each control area.

Finally, some jurisdictions have developed their own cyber security guidance, like the UK's Cyber Essentials and Essentials Plus. This is a self-assessment process UK companies can complete covering five controls for Essentials and adding in penetration testing for Essentials Plus.⁸

Selected Controls

Due to the condensed taxonomy and relative high rate of adoption, we selected the CIS Top 20 controls taxonomy as the nomenclature for the controls that we modelled in this report. A new version, v8 of the CIS taxonomy, now a Top 18 was made available in May 2020, but due to the timing of this project, work was completed using the v7.1 taxonomy.⁹ Further, we have selected just four controls as candidates for modelling, see below Table 6.

⁴ (MITRE 2020)

⁵ (CIS 2019)

⁶ (AICPA n.d.)

⁷ (Cloud Security Alliance 2020)

⁸ (National Cyber Security Centre n.d.)

⁹ (CIS 2020)

¹ (NIST 2021)

² (NIST Joint Task Force 2020)

³ (ISO n.d.)

Table 6: Summary of Selected Controls for Further Research and Modelling with Definitions (Source: CIS Top 20).

Category	Controls	Sub-Control	CIS Top 20 Definition
Basic	3 Continuous Vulnerability Management	Sub 1: Vulnerability Scanning	Continuously acquire, assess, and take action on new information in order to identify vulnerabilities, remediate, and minimize the window of opportunity for attackers.
		Sub 2: Automated Patching	
Basic	5 Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers	Sub 1: Configuration Management and Control Process	Establish, implement, and actively manage (track, report on, correct) the security configuration of mobile devices, laptops, servers, and workstations using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.
Foundational	8 Malware Defences	Sub 1: Anti-malware Implementation	Control the installation, spread, and execution of malicious code at multiple points in the enterprise, while optimising the use of automation to enable rapid updating of defence, data gathering, and corrective action.
		Sub 2: Anti-malware Configuration	
Organisational	19 Incident Response and Management	Sub 1: Incident Response Design	Protect the organisation's information, as well as its reputation, by developing and implementing an incident response infrastructure (e.g., plans, defined roles, training, communications, management oversight) for quickly discovering an attack and then effectively containing the damage, eradicating the attacker's presence, and restoring the integrity of the network and systems.
		Sub 2: Incident Response Standards	

Control 3: Continuous Vulnerability Management

For this control, we focus on Vulnerability Scanning and Automated Patching sub-controls. Only about 2-5% of CVEs have exploits published within 1 year.¹⁰ Less than 10% of vulnerabilities account for more than 90% of the attacks.¹¹ CVEs can be forecasted by CPE and CVSS to aid in model parameterisation and security controls planning.¹² The newly developed Exploit Prediction Scoring System (EPSS) estimates the probability that a vulnerability will be exploited based on its inherent characteristics.¹³ Scanning for vulnerabilities along with prioritising patching vulnerabilities with known exploits can reduce risk.

Control 3 could reduce the likelihood of an attack from ever occurring if commonly exploited vulnerabilities are remediated. It can also reduce the severity of an impact by limiting the number of machines exposed if partial remediation has been implemented.

Control 5: Secure Configuration for Hardware and Software

Common misconfigurations include: default/out of the box account settings (i.e., usernames and passwords), unencrypted files, web application and cloud misconfiguration.¹⁴ 82% of vulnerabilities are misconfigurations, with 73% of organisations having at least one critical security misconfiguration exposing critical data and systems. While “93% of cloud deployments had some misconfigured cloud storage services”.¹⁵ Human error is the most likely cause of misconfiguration, as was case in the recent Facebook outage.¹⁶

Control 5 could reduce likelihood of an attack from ever occurring if common misconfigurations are addressed. Also reducing the severity of the number of machines exposed if partial configuration issues has been addressed.

¹⁰ (Householder et al., n.d.)

¹¹ (Allodi 2015)

¹² (Leverett, Rhode, and Wedgbury 2020)

¹³ (FIRST 2021; Jacobs et al. 2021; 2020)

¹⁴ (Louerio 2020)

¹⁵ (Greig 2020)

¹⁶ (Janardhan 2021)

Control 8: Malware Defences

For this control, we focus on Anti-malware Implementation and Anti-malware Configuration sub-controls. There are different types of anti-virus/anti-malware: behavioural, heuristic, machine learning/AI. Leading advice is to deploy more than one industry standard anti-virus solution or to provide air-gapped media scanning stations. The effectiveness of anti-virus products in detecting malicious software ranged from 90% to 98%.¹⁷ Yet, anti-malware “performance was found to be lower under real-life conditions compared to tests conducted in controlled conditions.”¹⁸ Malware is always evolving and changing over time and now does not necessarily use traditional executables caught by anti-malware software to carry-out its activities.¹⁹

Control 8 is likely to reduce the likelihood of an attack from occurring if known malwares are blocked. While it will also reduce the number of machines exposed if an attack is limited in its propagation within the organisations network.

Control 19: Incident Response and Management

For this control, we are focused on Incident Response Design and Incident Response Standards sub-controls. There are numerous benefits of incident response

plans such as improved decision making, better internal and external coordination, unity of effort and limit of financial loss. Conducting a premortem might help reduce the “tunnel vision.” Integrating Incident Response Teams and Security Management teams can aid in organisational learning.²⁰ Scenario-based training approach for incident response teams may help overcome performance barriers.²¹ While researchers have reviewed what components comprise effective corporate communication during and following an attack.²² Further, war-gaming a cyber event on a regular frequency can help ensure organisational resilience during a real threat.²³

Control 19 could affect likelihood as compliance to a security standard may help push improvements in other controls that will help reduce the likelihood of an event ever occurring. It will also impact severity, reducing the number of days of outage or interruption for the malware and cloud outage scenarios and reduces the number of records breached for the data breach scenario.

Control Insights for Case Study Companies

BitSight can observe and, in some cases, infer the current state of each of these controls strategies for

²⁰ (Ahmad et al. 2020)

²¹ (O’Neill, Ahmad, and Maynard 2021)

²² (Knight and Nurse 2020)

²³ (Bailey, Kaplan, and Weinberg 2012)

Table 7: Cybersecurity Controls Baselines for Case Study Companies (Source: BitSight).

Controls	Sub-Control	Transportation	Apparel Retail	Manufacturing
3 Continuous Vulnerability Management	Sub 1: Vulnerability Scanning	Needs improvement	Acceptable	Needs improvement
	Sub 2: Automated Patching	Needs improvement	Acceptable	Needs improvement
5 Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers	Sub 1: Configuration Management and Control Process	Needs improvement	Needs improvement	Needs improvement
8 Malware Defences	Sub 1: Anti-malware Implementation	Acceptable	Acceptable	Acceptable
	Sub 2: Anti-malware Configuration	Acceptable	Acceptable	Acceptable
19 Incident Response and Management	Sub 1: Incident Response Design	Needs Improvement	Acceptable	Needs Improvement
	Sub 2: Incident Response Standards	Needs Improvement	Acceptable	Needs Improvement

Table 8: Cybersecurity Controls Modelling Parameter Impacts by Case Study Company (Source: CCRS Analysis).

Controls	Sub-Control	Impact	Ransomware		Data Breach		Cloud Outage	
			Likelihood	Severity	Likelihood	Severity	Likelihood	Severity
3 Continuous Vulnerability Management	Sub 1: Vulnerability Scanning	<u>Vulnerabilities</u> are more efficiently and frequently scanned with dedicated tools and procedures Likelihood: reduces the chance of an attack from ever occurring if commonly exploited vulnerabilities are remediated	X		X			
	Sub 2: Automated Patching	Improvement of the patching management system Severity: reduces the number of machines exposed if partial remediation has been implemented	X	X	X	X		
5 Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers	Sub 1: Configuration Management and Control Process	The focus is on the prevention from exploiting vulnerable services from a <u>security</u> perspective Likelihood: reduces the chance of an attack from ever occurring if common misconfigurations are addressed Severity: reduces the number of machines exposed if partial configuration issues have been addressed	X	X	X	X		
8 Malware Defences	Sub 1: Anti-malware Implementation	Implementation of an efficient anti-malware system Severity: reduces the number of machines exposed if attack is limited in its propagation	X	X		X		
	Sub 2: Anti-malware Configuration	The presence of an effective configuration influences the likelihood of an attack (pre-event control) Likelihood: reduces the chance of an attack from ever occurring if known malware is blocked	X					
19 Incident Response and Management	Sub 1: Incident Response Design	Implementation of a robust response to an attack (ex-post) Severity: reduces the number of days of outage or interruption for the malware and cloud outage scenarios and reduces the number of records breached for the data breach scenario		X		X		X
	Sub 2: Incident Response Standards	Compliance to the standard of the security Likelihood: compliance to a security standard may help push improvements in other controls that will help reduce the likelihood of an event ever occurring	X	X	X	X		X

the case study companies, shown in the following table. A “Needs Improvement” is the lowest level of implementation, which “Acceptable” is the average or expected level, with “Excellent” reserved for the highest level of implementation.

Translating Controls to Modelled Impacts

We simulate the possible mitigations that would come from each of selected control. The mitigations affect either a key driver of the scenario models (i.e., the number of endpoints or the number of data records breached) or a directly impacted the cash flow items. For example, if we simulate that the control “xyz” might reduce the data breached by 5%, all the balance sheet voices that depend on the exfiltration surface

would be affected. On the other hand, the control “xyz” might directly reduce the shock on the cash flow and a concrete example might be a lower regulatory fine due to compliance with the rules.

In Risk Reduction by Scenario, Case Study Company, and Control., we propose an overview of the controls and the sub-controls that we consider for the mitigation strategies modelling, and we show the possible impact on both the severity (cash flow items loss modelling) and the likelihood.

We also assume that the three companies belonging to the sectors described in the previous sections have system weaknesses, allowing us to understand how effective control implementations would be in different cases.

Controls Solutions

Organisations implement control strategies through various solutions such as IT systems like a Patch Management System or by Governance procedures like Incident Response Plans. Some solutions enable more than one control like SCAP Based Vulnerability Management can be part of a strategy for Control 3 and Control 5 and System Configuration Enforcement Systems enables both Control 5 and Control 8.

In terms of the modelling risk reductions, shown later in the report, we reviewed three different methods. The first being a given IT strategy, i.e. I want to improve all the levels of controls by one level where possible. Another method explored was to look at the control effectiveness in terms of investments in detection, alerting and preventing. The final method was to look at implementation of a control solution for a given control. This method seemed the most tangible to execute as it focused on the potential risk reduction a specific solution will have. Further, we were able to gather statistics from vendors on the potential risk reduction possible from their IT systems, which is reflected in the modelling results via a range of potential gain, i.e. minimum reduction to maximum reduction possible. Finally, this last method was agreed to be the most straightforward to interpret for the reader. Thus, this report chose to focus on the impacts of individual controls in reducing risk and not on combination of controls.

Table 9: Control Solutions (Source: CIS).

Control Solution	Control 3	Control 5	Control 8	Control 19	Count of Controls per Solution
Log Management System/ Security Information and Event Management (SIEM)			x		1
Security Content Automation Protocol (SCAP) Based Vulnerability System	x	x			2
Patch Management System	x				1
System Configuration Baselines & Images		x			1
System Configuration Enforcement System		x	x		2
DNS Domain Filtering System			x		1
Endpoint Protection System			x		1
Incident Response Plans				x	1
Count of Solutions Per Control	2	3	4	1	

5 Ransomware Scenario



Business Risk Overview

Computer malware – a virus, worm, or trojan – that can replicate and spread through IT networks is a long-standing cyber threat. The latest generations of malware can penetrate even the most secure corporate networks and paralyse IT systems by exploiting little-known vulnerabilities in security systems. This malware can have various payloads, but this scenario focuses on a ransomware payload which locks down critical systems. Recent developments in this space show attackers deploying multi-faceted extortion methods and threatening to disclose key corporate data, completely wipe, or corrupt the integrity of key data and software.

Threat Background

Ransomware is a type of payload delivered in malware which typically exploits a known or unknown vulnerability (zero-day) within a key platform or application. These vulnerabilities are tracked by the National Vulnerability Database (NVD) maintained by the US Department of Commerce, NIST.¹ Common Vulnerabilities and Exposures (CVEs) are assigned ID if they require public coordination and tend to be given to software flaws, rather than configuration errors. CVEs can be forecasted by Common Platform Enumeration (CPE) and Common Vulnerability Scoring System (CVSS) to aid in model parameterisation and security controls planning.² Only about 4% of CVEs have exploits published within one year of being made public.³ Common Weakness

Enumeration (CWEs), CVSS score and how recent CVEs are published make them more vulnerable to exploits. Vulnerabilities with known exploits have a median time to publication of 2 days and a mean of 91 days.⁴

There have been several high-profile ransom events targeting individual companies such as the Colonial Pipeline event in May 2021 and the JBS Food event in June 2021. However, more systemic events have the potential to cause the greatest total losses on a national or international scale. The most notable systemic ransomware event of 2021 had been the attack on Kaseya, an IT software vendor that allowed hackers to access many other corporate networks, thus expanding their reach and resulting in a ransom demand of \$70 million.⁵ NotPetya and WannaCry seem like events of the past but they can tell us something interesting about the systemic exposure of companies to the threat and the potential losses from an event as shown in Figure 10.

Cyber threat actors are scaling their capabilities due to the new business model of Ransomware-as-a-Service, with some groups targeting corporates to ensure a large payment. Many other incidents of malware have been recorded over the past 30 years. Toolkits for sale on the black market make it easier for hackers to perpetrate new variants of malware, creating a Ransomware-as-a-Service environments.

¹ (National Vulnerability Database 2021)

² (Leverett, Rhode, and Wedgbury 2020)

³ (Householder et al., n.d.)

⁴ (Householder et al., n.d.)

⁵ (Duffy 2021)

Table 10: Ransomware Scenario Severity Levels.

L	Description	% of infected endpoints	Days of Disruption	Chance
L1	This level captures a random malware similar to WannaCry with a payload of ransomware, infecting a minimal number of computers (10%) and causing a small business disruption (3 days). This is only an availability impact. A kill switch is identified.	10%	5	Moderate Chance
L2	This level captures a random malware similar to WannaCry with a payload of ransomware, infecting a significant number of computers (25%) and causing a minor business disruption (5 days). This is only an availability impact. A kill switch is identified.	25%	10	Low Chance
L3	This level captures a targeted malware, with a payload of ransomware, infecting a substantial number of computers (50%) and causing major business disruption (10 days). This is only an availability impact. A kill switch is never identified.	50%	20	Unlikely
L4	This level captures a novel targeted malware with a payload of ransomware plus doxing, infecting a major number of computers (90%) and causing a lengthy business disruption (21 days). This is both an availability and integrity impact and you have to investigate what data was deleted and ensure that other data was not manipulated. A kill switch is never identified.	90%	40	Extremely Unlikely

Scenario Narrative

The IT networks of multiple companies are penetrated by a rapidly replicating ransomware virus that encrypts a large number of computers, servers, and industrial control systems, and disabling dependent business activities. The proportion of computers (endpoints) infected within the network of an organisation translates to the scale of disruption for the modelled corporate, while the number of infected organisations indicates counter-party risk.

A random, spray-and-pray tactic is used in the L1 and L2 levels, while L3 and L4 focus on a targeted attack. Targeted attacks try to break into corporate networks manually and attempt to cripple entire organisations instead of encrypting a spread of individual computers across multiple networks or systems using malicious email campaigns. Demands are made for cryptocurrency ransom payments to decrypt, but paying may not guarantee full restoration. Many other businesses are similarly affected, including suppliers and customers. Computer systems are initially disabled for a number of days. Other complications take months to resolve.

Metrics of Severity

The severity of the scenario is dependent on the proportion of computers (endpoints) infected within the network of the organisation while the number of infected organisations indicates the level of counter-party risk.

Scenario Severity Levels

Scenario levels allow for a sensitive analysis on the range of possible impacts facing an organisation and are detailed in Table 10.

Historical Precedents

The 2017 NotPetya virus – a contagious malware that locked computers and erased hard drives – infected the networks of 8,000 organisations, including several that issued profits warnings due to the resulting disruption to revenues, and direct costs of over \$10 billion. WannaCry, a similar virus infected 30,000 computers and led to losses over \$3 billion.

A.P. Moller-Maersk has revenues of \$35 billion, 88,000 employees, and operates across 130 countries.

In June 2017, Maersk IT networks were infected by NotPetya. Maersk was paralysed for nearly ten days, while it purged and rebuilt its IT infrastructure. The IT team reinstalled over 4,000 servers, 45,000 PCs, and 2,500 applications over a ten-day period. This was estimated to cost Maersk up to \$300 million purely in order to rebuild infected endpoints.⁶ Maersk has reported that its losses from the single infection event overall exceeded \$950 million.

How the Scenario Impacts the Case Study Companies

An organisation's IT network is compromised by the malware through a previously unknown ('Zero Day') vulnerability in its systems. It spreads through the network before activating and encrypting many priority servers and computers.

Business activities that depend on IT are disrupted for the time it takes to repair and restore the computer systems. Restoration time is a major variable in the business impact. The current computer chip shortage increases the time it takes to procure replacement systems. Counter-party organisations are also paralysed for similar periods.

Transportation Industry

Transportation companies are highly dependent on externally facing websites and services to reach customers interested in booking tickets. Disruption

to these services would directly cause revenue losses as consumers switch to available services provided by other companies. For this sector, we assert that the servers supporting these external websites have the greatest revenue dependencies. Vulnerabilities are exploited on these servers to enable the attack resulting in extended outages as the company navigates event recovery.

Apparel Retail Industry

Apparel Retail companies have mixed dependency on external facing websites and endpoints within individual stores such as tills. For this scenario, we imagine servers are doing the heavy lifting for both types of endpoints and thus are the underlying endpoint with the greatest revenue dependency. Vulnerabilities are exploited on these servers to enable the attack resulting in extended outages as the company navigates event recovery.

Manufacturing Industry

As has been seen in a growing number of industrial ransom events (Colonial Pipeline and JBS in this year alone), we imagine the attack affects plant floor production, directly exploiting vulnerabilities in HMIs (Human Machine Interface Devices). This results in production outages for the duration of the event and requires the company to implement production line start-up procedures, steadily ramping up production to full capacity after a period of outage.

⁶ (Palmer 2019)

Figure 10: Companies Impacted by NotPetya Ransomware Event in 2017 (Source: CCRS Analysis).

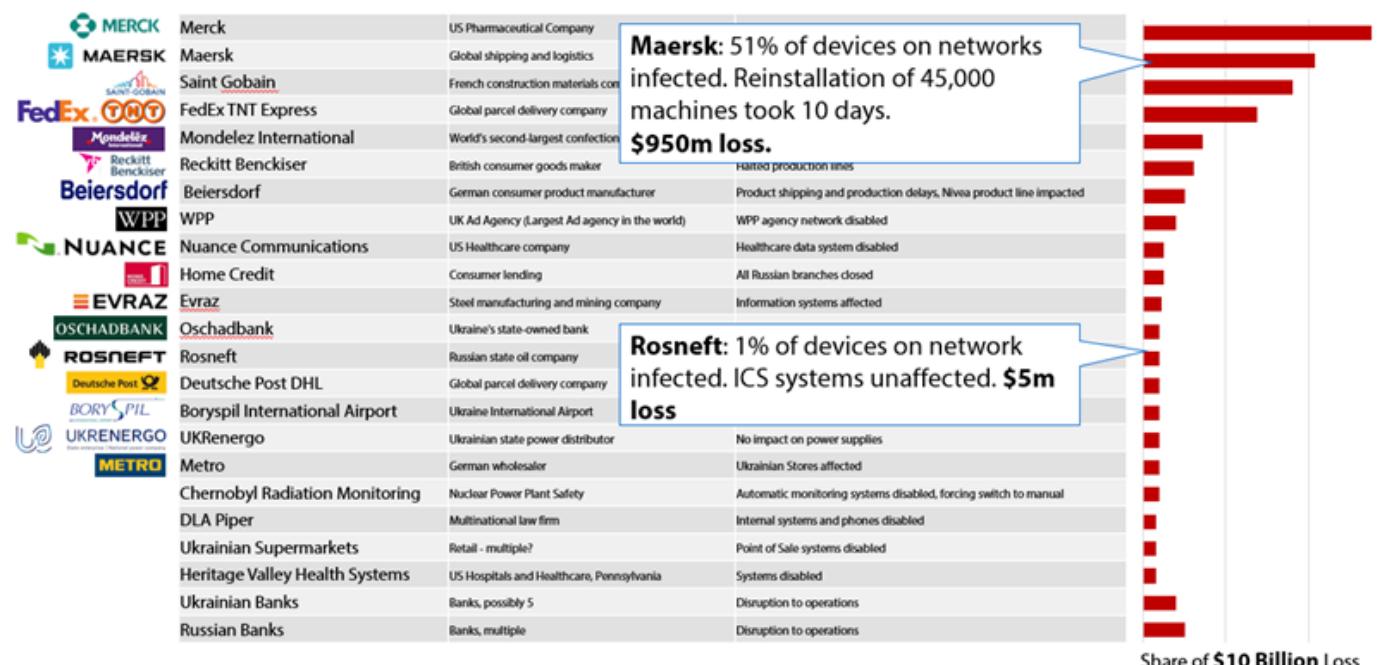


Table 11: Ransomware Scenario Cash Flow Impacts by Case Study Company (Source: CCRS Analysis).

Cash Flow Category	Cash Flow Element	Impact	Transportation Company	Apparel Retail Company	Manufacturing Company
Revenue Shock	Revenue	Business interruption resulting from lack of access to data or workstations.	X	X	X
Routine Costs Shock	Labour Costs	Internal labour costs to rebuild systems.	X	X	X
	Marketing and PR	A minor marketing and PR cost will be included to combat any reputational damage following the event.	X	X	X
	Data Software and Maintenance	Increase in internal maintenance and software costs to prevent future events, including additional employee training and access management.	X	X	X
Non-Routine Costs Shock	Impairment on PPE	External consultant costs to reconstruct any lost data and rebuild from backups AND cost to purchase new equipment for those considered to be a complete loss.	X	X	X
	Incident Response Costs	Direct costs incurred to negotiate ransom payment; conduct forensics investigation; purchase decryptor tools and additional legal fees related to project management.	X	X	X
	Legal Settlements	D&O litigation brought by shareholders in response to the financial impact of the event will be included and a consumer class action relating to the data breach explored in the L4 variant as a part of a doxing event.	X	X	X
	Regulatory Investigation and Fines	This cost is the fine applied by EU's Data Protection Authorities for GDPR fines. Other jurisdiction fines will be explored.	L4 only	L4 only	L4 only
	Compensation Costs	This is the average consumer compensation for the data breach event explored in the L4 variant, the average severity is estimated based on the type of data (PII, PCI, PHI).	L4 only	L4 only	L4 only
	Ransom Payments	Ransomware payments will be explored in the modelling but will not be the driver of the loss.	X	X	X

Modelling Methodology

Cash Flow Impacts

The above table summarises the cash flow categories impacted by the ransomware scenario with a description of the impact and impacts broken down by case study company. Two of the categories of impact only apply to the L4 level modelled.

Modelling Overview

This model is based on two key drivers of loss:

- The number of infected endpoints
- Duration of outage impact

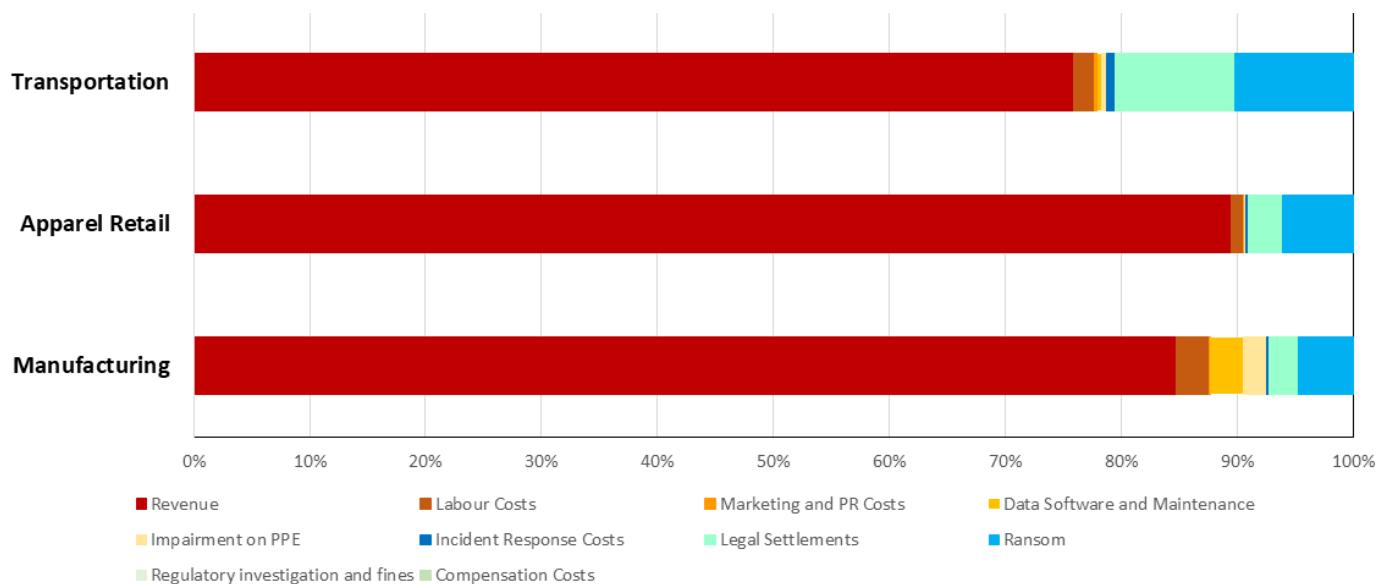
The model depends on estimates of potentially vulnerable host populations of machines across each

case study company's IT systems. We have estimated each IT system based on observations of the number of employees, number of stores/shops/facilities and publicly available disclosures in annual reports, along with data provided by BitSight. Likely populations of key operating system and application software products are also estimated for each machine type. This is currently based on typical industry usage estimates. The relative vulnerability of these different software products is estimated based on the rates and severity of historical vulnerabilities and exploits. We assume a revenue dependency per endpoint based on characteristics of each case study sector.

We assume a distribution of outage duration from 5 to 40 days for the portion of the business dependent on those infected endpoints. Successful ransomware

Table 12: EV@Risk Results – Ransomware (Source: CCRS Analysis).

Case Study Company	EV@Risk 5yr, \$ millions (L1 to L4 Losses)	EV@Risk % Loss	Weighted Average Expected Loss 5 yr, \$ millions	Weight Average Expected % Loss
Transportation	\$7.24 to \$1,162.66	0.12% to 18.70%	\$42.01	0.68%
Apparel Retail	\$22.95 to \$2,969.71	0.06% to 7.73%	\$174.86	0.23%
Manufacturing	\$27.26 to \$2,532.25	0.11% to 10.67%	\$87.32	0.74%

**Figure 11: Decomposition of 5 year EV@Risk Results by Cash Flow Category for Ransomware Scenario for L2 (Source: CCRS Analysis).**

attack events range in duration from 1 day to 60 days, with a most likely duration of 23 days.⁷ Data shows that hackers can spend significant time in corporate networks doing reconnaissance before they execute an attack, in one case a hacker was present in an corporate system for 13.5 days before carrying out an attack.⁸ All this could possibly justify an increase the outage duration beyond the current maximum of 40 days.

We have analysed a database of ransom payments made to known Bitcoin wallets associate with several key variants of malware.⁹ This data analysis begins

in 2010. The highest ransom payments in since this start date are in between \$2m and \$6m USD.

For the L4 variant where a data breach occurs via a doxing attack (ransom and data breach attack), we assume a modest data breach, resulting in GDPR Fines, Compensation Costs, and a Class Action Lawsuit.

BitSight has found that there is an increased likelihood for ransomware events at organisation with lower BitSight scores, thus it is assumed that the Transportation and Manufacturing Case Study Company experience higher likelihoods of attack when compared to the Apparel Retail Company.¹⁰

⁷ (Kivu and Hiscox 2020)

⁸ (Kivu 2020)

⁹ (Concinnity Risks 2021)

¹⁰ (Cadet 2021)

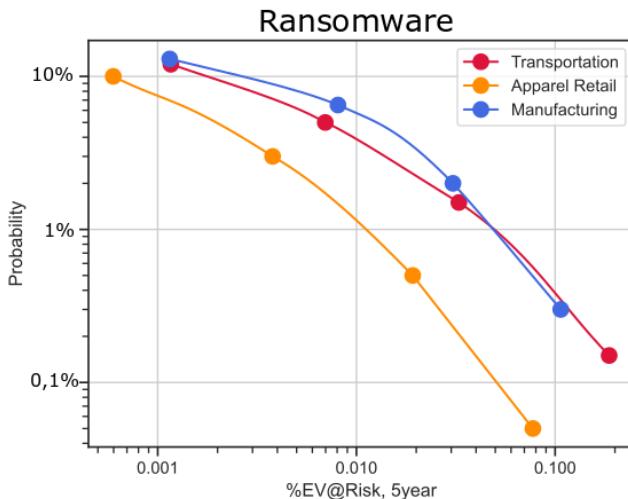


Figure 12: Ransomware Impact Overview by Level and Case Study Company (Source: CCRS Analysis).

Scenario Loss Results

The following table summarises the scenario modelling results. The first column shows the total financial impact of the scenario for L1 to L4 levels modelled. The middle column shows the % of the EV baseline each of those L1 to L4 level results in the left column represent. Finally, the last column shows the weighted average expected EV@Risk over the next 5 years, meaning it is the multiplication of the EV@ Risk and probability for each level modelled as well as the weighted average of all levels modelled.

The primary cash flow category of loss is revenue while ransom payment is the secondary category driving the losses for the Ransomware scenario. In the L4 variant, compensation costs and legal settlements overtakes the ransom payment as the secondary driver of losses due to the added data breach from the doxing event.

Risk Mitigation Results

For each control we propose two variation bounds: a minimum and maximum risk reduction to deal with the uncertainty in estimate this potential risk reduction. The following table shows the range of percent risk reductions in the expected weighted average EV@Risk from cybersecurity control implementation.

Transportation sees the greatest risk reduction from improving their malware defences (Control 8) while Apparel Retail and Manufacturing see the greatest reduction from configuration management improvements (Control 5).

Table 13: Ransomware Risk Reduction Results (Source: CCRS Analysis).

Control	Transportation	Apparel Retail	Manufacturing
Control 3	6 to 47%	4 to 34%	9 to 22%
Control 5	3 to 47%	6 to 48%	7 to 51%
Control 8	11 to 52%	5 to 43%	10 to 49%
Control 19	4 to 27%	4 to 19%	6 to 27%

Conclusions

A ransomware event can cause significant damage to corporate cash flow positions, with restoration from such an event a major variable in the modelling. For the Manufacturing company we assume that the malware infects their HMIs, while for the Transportation and Apparel Retail companies we assume that it infects their key servers. Thus, the Manufacturing company is the most impacted by the ransomware event given the revenue dependencies of their HMIs

The primary loss driver for this scenario is from outage-related revenue losses. The secondary driver for losses in the most extreme variant is the added doxing event, a growing trend to ensure victims pay the ransom. Additional costs would come from forensics and incident response, data reconstruction, media management, and equipment damage.

6 Data Breach Scenario



Business Risk Overview

Loss of confidential data that breaches the privacy of customers, employees, clients, or counter-parties, has proven damaging to many businesses, with costs of incident response, notification and compensation, regulatory fines, litigation settlements, and reputational damage and loss of customers. Data breaches are caused by accidents, cyber attacks, and the work of malicious network insiders.

Threat Background

A cyber attack carried out by external hackers can result in a considerable business impact due to the theft of large amounts of sensitive data. Many sectors have come under attack and suffered a data breach in recent years. Among them are sectors with a strong exposure to the web for both internal and external trade, or those that have historically been the most vulnerable (e.g., the health and education sectors). Industry reports identify several system vulnerabilities that vary from sector to sector.¹ The most interesting key insights from these reports are:

- Phishing and stealing credentials (or hacking) were the most popular actions utilised in the security breaches in 2021.²
- Across the variety of actions for which data was captured by Verizon Media, hacking amounted to 25% of data breaches or losses, malware was used in 10% and human error was responsible in 20% of cases.⁵²

- The use of malware appears to be decreasing consistently as a tool in data breaches. This is due to its replacement by other types of attacks like hacking or social engineering. Human error remains a growing risk associated with data breaches.

We report the proportion of identified tactics, techniques, and procedures in Figure 13.

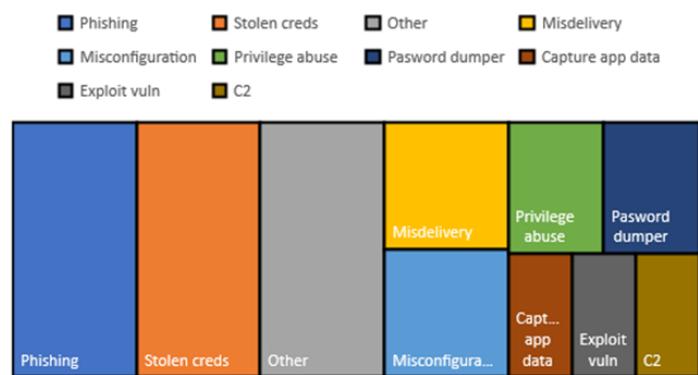


Figure 13: Relativities of Threat Actions for Data Breaches (Verizon, 2021).³

Scenario Narrative

A cyber attack by external hackers with insider help results in the theft of large amounts of sensitive data, including customer personal details, credit card information, health records, financial information, supplier contracts, intellectual property, and other records. The company follows procedures for reporting the loss to regulators, notifying those affected, and paying compensation. The resulting

¹ (Verizon 2021)

² (Verizon 2020)

³ (Verizon 2021)

Table 14: Data Breach Scenario Severity Levels.

L	Severity Level Description	Data Breach	Size of Data Breach			Chance
			Transportation	Apparel Retail	Manufacturing	
L1	Reduced: The cyber attack manages to capture a few tens of thousands of data among customers and company employees. <i>Type of data: PII data only.</i>	Significant	80,000	500,000	Hundreds of data	Significant Chance
L2	Moderate: The cyber attack manages to capture a few hundreds of thousands of data among customers and company employees. <i>Type of data: PII data only.</i>	Major	600,000	3,000,000	1,000	Moderate Chance
L3	Severe: The cyber attack manages to capture a few millions of data. <i>Type of data: PII and PCI</i>	Severe	3,000,000	15,000,000	5,000	Low Chance
L4	Comprehensive: The cyber attack manages to capture tens of millions of data. <i>Type of data: PII and PCI</i>	Comprehensive	8,000,000	60,000,000	22,000	Unlikely

negative media harms the business reputation, reducing customer sales and impacting share price.

- Transportation industry data breach: For a transport company this translates essentially into an “attack” on the credibility the business relies on and the general “market value” of the provided products. Transport companies nowadays make an extensive use of booking platforms to provide their service to the travellers. They treat a large amount of personal and credit related data.
- Apparel Retail industry data breach: For the retail sector there has been a substantial change in the last decade from Point of Sales (PoS) to web attacks. This is due to the extensive migration of the core business (sales) of the companies to e-commerce. The nature of data that are provided on-line by the customers, motivates the attackers to target credit-related data (PCI) for financial reasons. However, also personal data are at risk around at the same level of credit data

- Manufacturing industry data breach: The manufacturing industry is highly prone to external attacks by organised groups of hackers. These often take the form of ransom demands, but the sector is particularly sensitive to technological/manufacturing espionage.

Metrics of Severity

We develop the data breach scenario around the following three main characteristics:

- The volume of data lost
- Data type differentiation
 - PII (Personally Identifiable Information)
 - PCI (Payment Card Industry)
 - PHI (Protected Health Information)
- Characteristics of the industry

The volume of data lost or “under attack” is meaningful in understanding the technical and the economic impact of the breach.

It is important not to focus on solely what past data on breaches demonstrates about the trend, as these data are not a reliable source for determining future breach traits for several reasons. Firstly, the past is often not informative for unique events such as a data breach linked to a catastrophic scenario (extreme events are modelled in the L₃ and L₄ scenarios). Secondly, the official statements of companies which claim data breaches should be taken with caution. It is well known that only the minority of attacks have been declared and are publicly known. As regulations and penalties in case of missing or untimely declarations have become more stringent in recent years, we can reasonably assume those public statements that have been made in recent years are more reliable than those published or indeed, not published, in years previous. We must also be cognizant of the role that time plays in bringing information on breaches to light: a data breach can only lead to the quantification of an economic loss after a few years, when statements may be released days or weeks after discovery. The vast majority of the economic loss is related to lawsuits and refunds may require several years of proceedings before leading to a summary judgement.

Scenario Severity Levels

We present four severity levels for the data breach scenario. From scenario L₁ to scenario L₄ we use an increasing level of loss intensity but a lower probability of occurrence. We report the description of the severity levels for the data breach scenario in Table 14.

There are essentially two drivers which determine the extent of a data breach: the number of exfiltrated data and the type of data (PII, PCI, PHI) stolen. The number of data records for each company is representative of the amount of data that they hold.

Historical Precedents

Respectively for the transport, apparel retail and manufacturing sectors, we provide a list of data breach events in recent years.

How the Scenario Impacts the Case Study Companies

Transportation Industry

In the transportation industry, breach attacks mostly target web applications and their databases due to the presence of customers critical information in those systems. Both PII and PCI data are at risk, though PCI data presents a higher challenge to strategic planning and hacking capabilities to exfiltrate. Errors caused by employees and social engineering leaks

are among the main sources of data breach in the industry. On the actors' side, the main motivations are largely financial.

- The large number of customers that transportation companies have access to make them extremely attractive to hackers. If a data breach attack manages to penetrate the company's servers or applications, it is highly likely that a large amount of data can be exfiltrated.
- Internal errors are among the main weaknesses for large companies with thousands of employees since it increases the risk of error and training costs.
- Customer bookings in the transport sector are made through online platforms or applications. Booking management is often delegated to external entities. These have been vulnerable in the past and are exploited by attackers often.
- Past data breach events (mostly involving airways companies) revealed poor control and identification system. Competent authorities like ICO have repeatedly intervened with some of the heaviest penalties in the industry.
- The costs relative to securing hardware and software, backups and applications are often substantial considering the amounts of data handled.

Apparel Retail Industry

The greatest damage that a retail company will incur from a data exfiltration attack is to their reputation and market position. A successful data exfiltration would present as a direct attack to the customers of the company – online sales presuppose the collection of personal and credit card information to proceed with orders. In the light of these considerations, compensation costs may be extremely disruptive, particularly considering that half of the exfiltrated data is likely to be credit-data.

- 2020 and 2021 have been crucial years for online business, and the number of sales made online grew significantly due to the pandemic. This trend increases the attraction for the attackers seeking private financial details.
- For international businesses, the pervasive presence of PoS technology, the amount of data to be managed and the distinct contingencies of different countries may all create weaknesses to breaches, as the attack surface is very wide.

Table 15: Summary of Significant Historical Data Breach Events by the Sectors of the Case Study Company.

Transport 	Apparel Retail 	Manufacturing 
<ul style="list-style-type: none"> ● Star Alliance (2021) <ul style="list-style-type: none"> ○ Highly sophisticated attack on SITA servers that exposed the data of hundreds of thousands of passengers ○ A first estimation reveals about 2,00 million travellers affected ○ Declarations show that no sensitive data were stolen other than passengers' names, tier status and membership number ● easyJet (2020) <ul style="list-style-type: none"> ○ Sophisticated cyberattack affected 9,00 million customers ○ 2,208 customers had credit/debit card details accessed (PCI) ● British Airways (2018) <ul style="list-style-type: none"> ○ Around 420,000 customers affected ○ Both customers and staff were the victims of the exfiltration ○ Around 244,000 customers had credit/debit card details accessed (PCI) ○ Compensation costs for the victims estimated around £2.4 billion (average per victim around £ 2,000) ○ ICO fines estimated around £20,00 million with an initially planned sum of £183,00 million ○ £20,00 million is still the highest fine issued by the ICO ● Air Canada (2018) <ul style="list-style-type: none"> ○ Air Canada app was affected by a data breach with the consequent loss of thousands of personal customers details ○ According to the company declarations no credit card data were exfiltrated ○ Several types of PII data have been at risks like passenger's passport details, nationality, and birth date ● Cathay Pacific (2018) <ul style="list-style-type: none"> ○ In March 2018 around 9.4m of passengers' data were exposed to attack ○ The event was made public six months later ○ In March 2020, ICO announced a £500,000 fine for the company 	<ul style="list-style-type: none"> ● Target (2013) <ul style="list-style-type: none"> ○ PoS attack conducted in the stores (through a malware installation) ○ Third-party vendor attack ○ Around 70.00m of PII and 70.00m PCI data were stolen ● Home Depot (2014) <ul style="list-style-type: none"> ○ Third-party vendor attack ○ Attack conducted with a malware ○ Around 52.00m of PII and 56.00m PCI data were stolen ● eBay (2014) <ul style="list-style-type: none"> ○ Access through compromised employees' credentials ○ 145.00m PII data were stolen ● PNI Digital Media (2015) <ul style="list-style-type: none"> ○ The attack was probably due to the poor configuration of the system ○ Millions of PCI and PII data compromised ● Marriott Hotel (2018) <ul style="list-style-type: none"> ○ Both PII and PCI customers data were stolen from the databases of the company ○ The attack counts around 500.00m of customers exposed data ● Macy (2019) <ul style="list-style-type: none"> ○ Mix of PCI and PII customers data were compromised ○ The attack was made through the website of the company: a web-skimming attack 	<ul style="list-style-type: none"> ● Royal Dutch Shell (2010) (another attack confirmed in 2020) <ul style="list-style-type: none"> ○ 176,000 data stolen of employees ○ The data breach was perpetrated by internal employees ● LC Industries (2015) <ul style="list-style-type: none"> ○ Data breach of around 3700 customers records ○ Malware installed in one of the retail sites to capture customers information ● Hanes Brands (2015) <ul style="list-style-type: none"> ○ 900,000 customers records compromised ○ Attack perpetrated through the company website ● FACC (2016) <ul style="list-style-type: none"> ○ Email attack (whaling attack) ○ Attack estimated value around \$54 m ● Boeing (2017) <ul style="list-style-type: none"> ○ 36,000 workers' data under risk ○ No consequences for this incident ● Acer (2021) <ul style="list-style-type: none"> ○ REvil hackers attack through a vulnerability of an external provider server ● Quanta (2021) <ul style="list-style-type: none"> ○ REvil hackers' attack ○ \$50m ransom demanded

- Major retail companies have an extremely e-commerce-oriented business, where attacks can be geared towards collecting both personal and credit data:
- The retail sector stores a very high level of stolen credential data. These data are particularly profitable for the attackers as demonstrated by historical incidents.
- The presence of online platforms has triggered the development of attacks such as pretexting, i.e., the simulation of online environments to steal data: as reported by the literature, a key point lies in educating users and employees to be ready to disclose and report any anomalies.
- Reputational risk is among the most disruptive cost for a large retail company, especially considering investment-related costs such as the ones to rebuild the image and customer confidence.

Manufacturing Industry

In the manufacturing industry, malware is widely used by attackers to extract credentials and enter

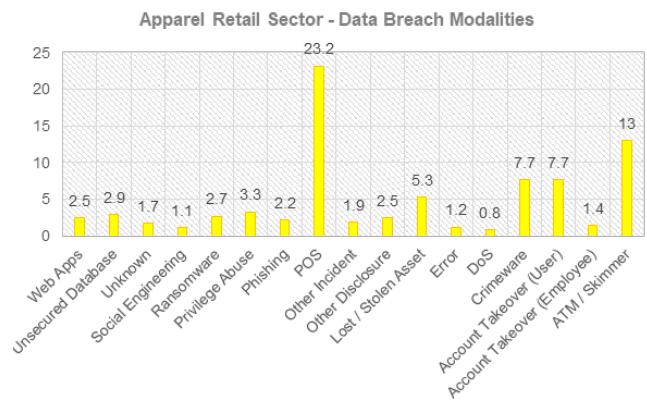


Figure 14: Data Breach - Exfiltration Methods
(Source: BitSight Internal Dataset, 2021).109

secure information systems. The risk of financial extortion is considerable, but cyber espionage and IP theft is also highly plausible and may have its own hugely disruptive effects.

After such an attack takes place, huge costs are accrued in pursuit of expert opinions and advice on negotiations, especially in the case of extortion of sensitive data on projects and technologies. Customers in the manufacturing industry are often not final consumers and so the risk of escalation

Table 16: Data Breach Cash Flow Impacts by Case Study Company.

Cash Flow Category	Cash Flow Element	Impact	Transport	Apparel Retail	Manufacturing
Revenue Shock	Revenue	Data breach impact on revenues due to possible loss of customers by companies. These costs follow economies of scale and depend on the size of the data breach	X	X	X
Routine Costs	Marketing and PR Costs	Cost related to the investments the company has to make to renew its image after a data breach is made public	X	X	
	Data Software and Maintenance	The costs of renewing computers and software after an attack	X	X	X
Non-routine Costs	Compensation Costs	The costs of compensating customers and staff due to exfiltrated data. Severity depends on type of data and sector	X	X	
	Other Costs	Under this voice we add up the costs of a data breach per datum that do not fall under the other cost categories. For example, compensation costs for customers outside of lawsuits, additional maintenance costs, business interruption costs etc. These costs follow economies of scale and depend on the size of the data breach	X	X	X
	Impairment on PPE	Devaluation of the company know-how	X	X	X
	Incident Response Costs	The costs of expert consultancy and technical support on the data breach	X	X	X
	Legal Settlements	Costs due to lawsuits. Four levels: Win, Settlement, Defeat and Major Defeat	X	X	X
	Regulatory investigation and fines	Costs due to fines imposed by regulators due to a data breach	X	X	X

along the production chain can entail serious costs in terms of reputation and legal issues. Attacks can affect extremely sensitive data for companies. For example, in the technology sector, this would impact the value of the affected company. Impairment cost shocks of large EPPs (Endpoint Protection Platform) are expected for the most severe scenarios.

Out of a pool of 386 companies analysed internally by BitSight⁴, the transport sector recorded the highest risk in terms of deviation from the average of all sectors (+7.25%). Apparel retail had a +1.3% deviation while manufacturing was about 17% less

⁴ (BitSight Internal Dataset, 2021)

Table 17: Data Breach Risk Reduction Results (Source: CCRS Analysis).

Case Study Company	EV@Risk 5yr, \$ millions (L1 to L4 Losses)	EV@Risk % Loss	Weighted Average Expected Loss 5 yr, \$ millions	Weight Average Expected % Loss
Transportation	\$25.8 to \$998.1	0.41% to 16.05%	\$88.91	1.43%
Apparel Retail	\$73.6 to \$1,979.6	0.31% to 8.34%	\$187.63	0.79%
Manufacturing	\$18.96 to \$227.38	0.08% to 0.96%	\$33.38	0.14%

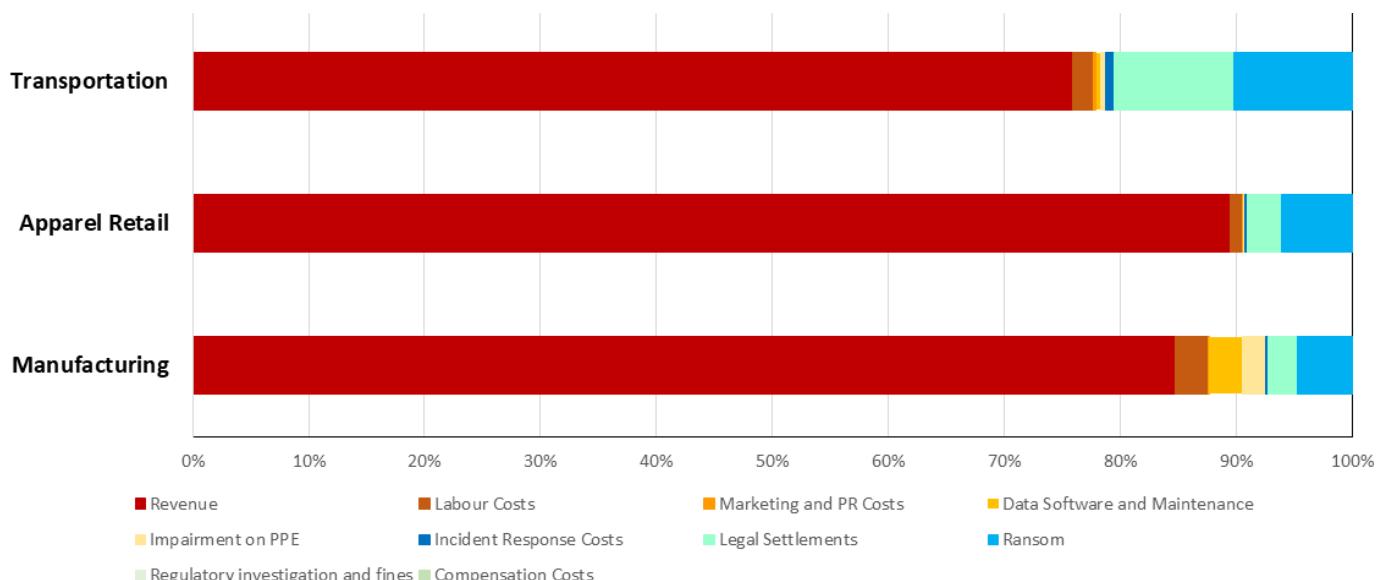


Figure 15: Decomposition of 5 year EV@Risk Results by Cash Flow Category for Data Breach Scenario for L2 (Source: CCRS Analysis).

risky than the other sectors. To conclude, Figure 14 shows the most sensitive attack modalities through which a data breach occurs in the apparel retail sector.

Modelling Methodology

The modelling part of a data breach scenario consists of mapping the magnitude and type of an attack into shocks to the different voices on a company's balance sheet. Each of the three case study companies modelled is generically associated with the real market and the sector to which it belongs. We tried to reproduce a data breach on the basis of qualitative and quantitative characteristics typical of the sector.

Modelling Methodology

The modelling part of a data breach scenario consists of mapping the magnitude and type of an attack into shocks to the different voices on a company's balance sheet. Each of the three case study companies modelled is generically associated with the real market and the sector to which it belongs. We tried to reproduce a data breach on the basis of qualitative and quantitative characteristics typical of the sector.

Cash Flow Impacts

Table 16 clarifies which cash flow items are impacted by a data breach for each company.

While the transport and the retail sectors suffer from the same balance sheet shocks, the manufacturing company losses are not retail oriented. Consequently, we do not consider a significant impact on marketing and PR or compensation costs for the manufacturing company.

To maintain comparability between companies, we choose not to include data breaches involving intellectual property. As we report in the next sections, this will have a significant influence on the impact of the manufacturing company.

Table 18: Data Breach Risk Reduction Results (Source: CCRS Analysis).

Control	Transportation	Apparel Retail	Manufacturing
Control 3	3 to 6%	6 to 34%	0.3%
Control 5	1 to 24%	4 to 27%	0.3%
Control 8	7 to 27%	8 to 27%	3 to 8%
Control 19	1 to 3%	4 to 5%	3 to 8%

Modelling Overview

The data breach model is based on two key drivers:

- The type of data that is stolen
- The size of the breach

These parameters provide a measure of the shock to the balance sheets of the companies chosen as case studies. In particular, the type of breached data Data

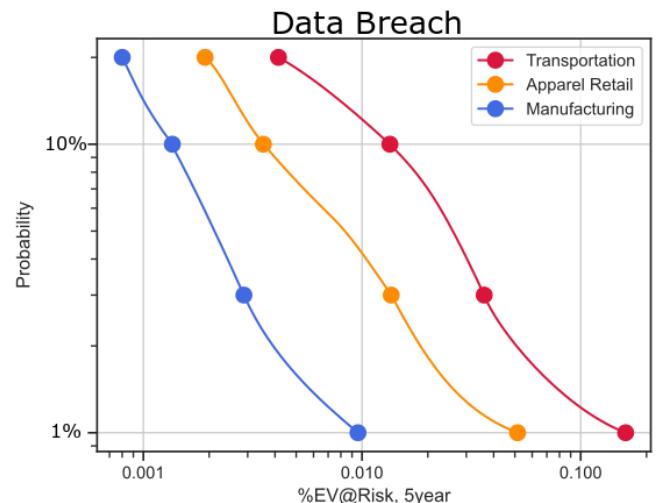


Figure 16: Breach Impact Overview by Level and Case Study Company (Source: CCRS Analysis).

defines the costs per datum and thus the impact on revenues, compensation costs and Impairment on PPE. The size of the data breach defines the severity of the four levels of the scenario (L1-L4).

To characterise the size of the data breach, we used proxies for the number of employees and the number of customers of the companies. This also indicates some diversity within the pool of selected companies (depending on industry characteristics).

The following costs, which do not directly depend on the characteristics of the data breach, are also modelled in the same scenario: marketing and PR costs, data Software and maintenance, incident response costs and legal settlements. These costs are also declined according to the level of the scenario (L1-L4) and their severity is the result of the joint work of several experts in the field. Regulatory investigation and fines are instead a cost based on the historical analysis of fines imposed by the regulator (GDPR).

Full details and data breach event numbers for the three case studies can be found in the Appendix section 'Data Breach Modelling Methodology Further Notes'.

Scenario Loss Results

The following table summarises the scenario modelling results. The first column shows the total financial impact of the scenario for L1 to L4 levels modelled. The middle column shows the % of the EV baseline each of those L1 to L4 level results in the left column represent. Finally, the last column shows the weighted average expected EV@Risk over the next 5 years, meaning it is the multiplication of the EV@ Risk and probability for each level modelled and then the weighted average of all levels modelled.

The primary cash flow category of loss is compensation costs while legal settlements and revenue losses are the secondary categories driving the losses for the Data Breach scenario.

In Figure 16 we present a general overview of the three companies.

Risk Mitigation Results

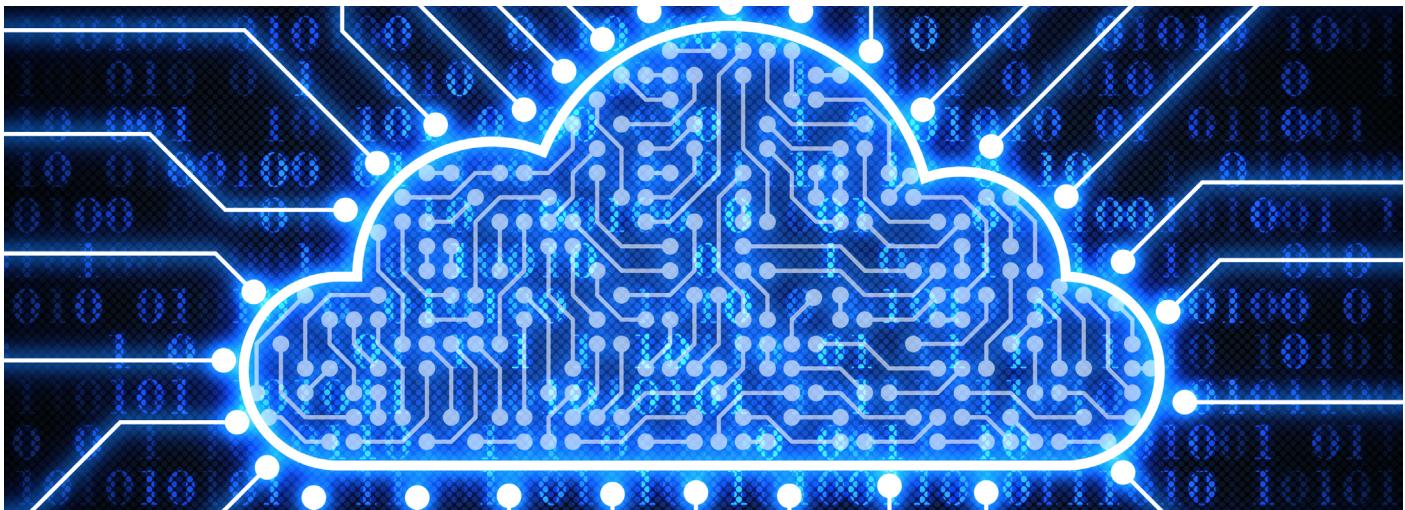
For each control we propose two variation bounds (min-max). We also report the corresponding results in terms of risk mitigation in Table 18.

Conclusions

A data breach is an extremely complex event to analyse both from a technical and economic perspective.

The objective of this section was to translate a four-level scenario (L1-L4) into an economic shock. We designed the event through three case studies of three companies belonging to different sectors (transportation, retail, and manufacturing sector). We incorporated these characteristics into the drivers (surface of exposure and data type) of the data breach and translated them into economic shocks. In the last part we simulated the role of possible mitigation strategies. We based our method on the analysis of controls (CIS) and translated their implementation into a range (min-max) of mitigation for each of the companies considered.

7 Cloud Outage Scenario



Business Risk Overview

Business systems that rely on public cloud services from a major CSP are out of action for the duration of the outage. These may include e-commerce, Software-as-a-Service, and services from third parties in your digital supply chain. This scenario provides an opportunity to assess cloud dependencies of business operations. Many organisations may not realise the degree to which their business operations are dependent on their cloud service provider.

Threat Background

Organisations are increasingly adopting cloud-based computing as an alternative to in-house systems. Cloud service providers have good reliability records but suffer occasional failures with systemic disruption potential to business systems and digital revenues. This scenario enables companies to review their cloud dependencies and assess losses that could occur to business operations during significant cloud outages.

Cloud is identified as a set of technologies for accessing services via the internet from any region of the world. The term “technology” here means a set of centralised computing resources such as servers, applications, services, and databases that are supplied by a provider. Cloud service is spread over different regions in the world and permits the connection to the service from everywhere. Whenever there is an issue with a specific connection, the cloud architect (that guarantees a certain degree of independence between regions) permits a re-connection to another region. This flexibility avoids extended service interruptions.

Technological growth permitted a boom in demand for this type of service. As a result, architectural requirements have evolved over time to accommodate different customer needs.

There are three main cloud provision models:

- Software as a Service (SaaS): software application with an interface fully controlled by the provider in the backend
 - Example: Dropbox - files storage directly controlled by the customers through the application
- Platform as a Service (PaaS): platform with integrated software supported by the provider
 - Example: Microsoft Azure - development environment that supports a tools and languages
- Infrastructure as a Service (IaaS): infrastructure access to computing, storage, and network resources
 - Example: Amazon Web Services - access to computing resources

In Figure 17 we report the spending forecast elaborated from Gartner.¹ As reported by the data, the technological future of companies seems to be increasingly linked to cloud services. For example, today any company that has computational needs, to manage external services, needs to interface with customers or needs to manage business with suppliers can go through cloud services without investing in hardware and software.

¹ (Costello and Rimol 2021)

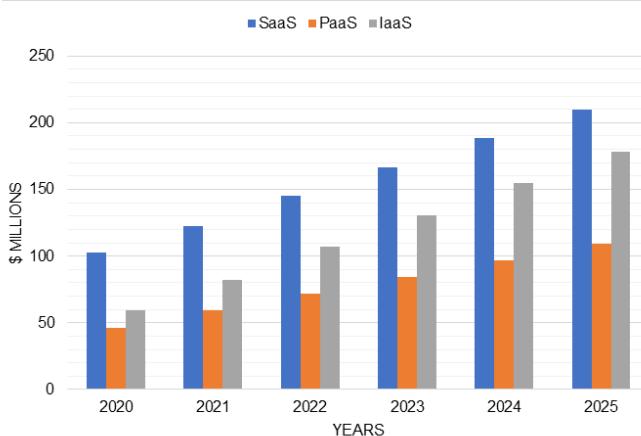


Figure 17: Market End-Users Share Forecasts, Expenditures \$ Millions (Source: Gartner Report, 2021).

But what is a cloud outage and why it is considered a cyber risk? A cloud outage is a downtime event during which all activities related to the provision of services via the cloud are forcibly suspended.

There are several risks behind cloud outage. A review of the current literature reports the following ones:

- Structural: technology-related causes such as problems with power supply systems, server problems, or undiagnosed errors
- Failures caused by external attacks: broadly speaking, any attack perpetrated by external hackers who decide to cause damage to servers, extract data from databases and cause a denial of service (DoS)
- Accidental errors: a large number of disruptions come from errors in the programming (configuration), maintenance, and testing in the cloud service
- Natural/environmental disruptions: natural events resulting in physical damage to data centres or the network

Cloud companies guarantee the functionality of the services, their maintenance, and updates. A failure of service leads to serious economic damage for the companies that use it. The interruption of service either directly damages the company's core business or its customers.

Cloud companies often manage to provide a continuous service to their customers thanks to the scalability of the different supply zones, see table below. However, there are exceptions and new types of error or possible vulnerabilities constantly emerge.

Table 19: Summary of Layers of Provisions within Cloud Architectures.

Layers of Provisions	Description
Regions	A physical location where data centres are located. Some providers offer centralised services in accordance with the region layer, some others have further sub-divisions that are generally independent. In this second case, a threat that hits a specific centre has less probability to affect others.
Zones	To avoid problems of continuity of service provision, a cloud provider can group centres into "zones". Zones by definition are more tolerant to the risks of failure of individual centres.
Local Zones	Are areas where services are provided for specific customers who base their business on particular characteristics of the connection (e.g., latency).
Replicability Across Regions	Some providers provide the ability to replicate their provisioning across different service centres. This allows to interchange the supply in case of disruption.

Scenario Narrative

A major cloud service provider suffers an outage of unprecedented scale and duration, affecting many of its services and cascading across several of its availability zones. Because of the technical complexity of the failure, it takes a long time to restore the service. All business processes that rely on these cloud services are unable to operate. Many other companies, including suppliers and customers that also use that CSP are impacted by the event.

Metrics of Severity

Risk calculation and business impact are computed on the basis of the following parameters:

- Number of providers offering services to the company
- Number of outages: within the considered time horizon (5 years) how many outages may affect a company
- Duration: number of hours during which the service remains offline

Table 20: Cloud Outage Scenario Severity Levels.

L	Services	Number of outages (within the next 5 years)	Duration (hours)	Chance
L1		1	6	Possible Chance
L2	For the computation of the risk, each company is impacted with regard to the providers that operates for that specific company. This computation is also weighted by the business that the company develops in each specific region. For other costs, variables such as reputation, hiring experts and consultants to solve technical problems, and litigation costs are considered in proportion to the level of risk.	4	12	Low Chance
L3		5	72	Very Unlikely
L4		10	96	Extremely Unlikely

- Number of data centres for each region where the company operates

- 9 June 2020, IBM Cloud⁵: third party networking failure. Issues with access to the environment for the customers.
- 17 July 2020, Cloudflare⁶: black bone network issue. Affected several parts of the world.
- 11 August 2020, Salesforce⁷: four hours outage in North America due to server problems.
- 24 August 2020, Zoom⁸: web and video access issues.
- 28 September, Microsoft Azure⁹: Microsoft 365 issues for US customers (login authentication). The main causes were related to code defect and tooling error.
- 7 October 2020, Microsoft Office 365¹⁰: update issue caused a general outage to the main Microsoft Office services.
- January 2021, Verizon¹¹: thousands of customers affected in the north-eastern US. The main cause was a software issue.
- 4-17 February 2021, Microsoft Teams: joining meetings issues in North America and South America.
- 17 February 2021, outage in Texas¹²: households electricity issues (blackout) for millions of people due to a windstorm.

⁵ (Sharwood and Editor 2020)

⁶ (Graham-Cumming 2020)

⁷ (Tsidulko 2020)

⁸ (Vincent 2020)

⁹ (Foley 2020c)

¹⁰ (Nichols 2020)

¹¹ (Goldman 2021)

¹² (Busby et al. 2021)

² (Foley 2020a)

³ (Ramel and 04/13/2020 2020)

⁴ (Foley 2020b)

- 3 March 2021, Verizon¹³: moderate disruptions for the customers in Northeast and Mid-Atlantic state.
- March 2021, Microsoft¹⁴: multiple Microsoft services went down (Azure, Office, Teams)
- April 2021, Microsoft¹⁵: DNS issues for Azure and Teams.
- 12 April 2021, Google¹⁶: Google Drive and other cloud-based apps had issues for around three hours due to a multiple service issue.
- 8 June, Fastly¹⁷: global outage that led to several issues to Reddit, Twitch, CNN, and The New York Times.
- 11 June, Microsoft¹⁸: Microsoft 365 and Microsoft Teams outage issues.
- 17 June, Akamai¹⁹: internet outages that caused several disruptions for different companies.

¹³ (Narcisi 2021a)¹⁴ (Warren 2021)¹⁵ (Abrams 2021)¹⁶ (Porter 2021)¹⁷ (Shead 2021)¹⁸ (ENow Software 2021, 365)¹⁹ (Narcisi 2021b)

- 4 October, Facebook: huge outage of around 6 hours of all Facebook's services²⁰
- 8 June, Fastly²¹: cloud outage due to misconfiguration that caused several disruptions to AWS and other big companies

How the Scenario Impacts the Case Study Companies

The main drivers of the scenario are essentially the location of the companies' business activities and the adoption of the cloud service and coverage of the territory.

Transportation Industry

The transport industry provides direct services to the customer. A cloud outage could have multiple effects both internal and external to the company. For example, an outage could lead to the interruption of the provision of booking services, which would have a direct impact on customers and the company's image, or an outage could impact logistics and the entire organisational infrastructure of internal information and security systems.

²⁰ (Kentik 2021)²¹ (Browne and Shead 2021)

Table 21: Further Could Outage Scenario Parameter Details.

Company	Key Driver 1: Number of Outages	Key Driver 2: Impacted Business and Regions (Proxy)
Transport		
L1	1	25% - Europe
L2	5	35% - Europe
L3	7	35% - Europe
L4	14	19% - Europe
Apparel Retail		
L1	1	14% - Americas
L2	4	23% - Asia
L3	6	10% - Asia
L4	15	12% - Europe
Manufacturing		
L1	1	20% - Asia and Africa
L2	4	20% - Europe
L3	6	20% - Europe
L4	16	15% - North America

The case study we have analysed follows a business developed in Europe with a strong market share directed at domestic flights. It relies on cloud services both for offering services to customers and for internal management operations.

Apparel Retail Industry

As with the transport industry, the retail industry offers its products through online stores directly to customers. The case study analysed has an international market that develops production in Asia and has physical stores all over the world with a large share dedicated to the European market.

The company entrusts an important part of the market to the cloud as well as a lot of internal management (e.g., logistics). However, it can diversify through physical stores.

Manufacturing Industry

The analysed case study considers a company with about two thirds of the market in America and one third in Europe with a type of business oriented to other companies (i.e.: business to business). The number of customers is lower than in the other two companies but the margins on the product are very high. This allows greater mobility in diversifying the customer base. A large part of the internal management and information systems are managed through the cloud.

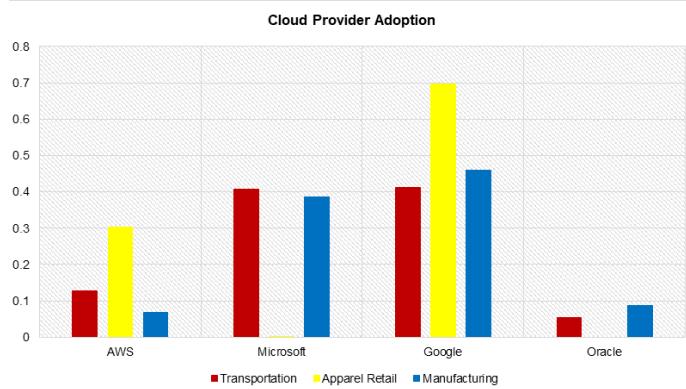


Figure 18: Cloud Provider Adoption (Source: BitSight).²²

BitSight's²³ internal analysis of the specific sectors in the case studies shows high cloud usage: the transport sector is around 80%, apparel retail 81% and manufacturing 78%. Among the providers considered, the transport company relies mainly on Google Cloud and Microsoft Azure and to a minor extent on AWS and Oracle. The apparel retail company relies most of its cloud activities on Google Cloud and AWS. The manufacturing company relies heavily on Google Cloud and Microsoft Azure and to a lesser extent on AWS and Oracle. In Figure 18 we show the cloud service adoption for the three companies.

²² (BitSight Technologies 2021a)

²³ (BitSight Technologies 2021a)

Table 22: Cloud Outage Cash Flow Impacts by Case Study Company.

Cash Flow Category	Cash Flow Element	Impact Description	Transportation	Apparel Retail	Manufacturing
Revenue Shock	Revenue	The revenue impact of cloud outage is found in the lack of access to services by the company and its customers. It directly depends on the number of outages that occur over time, location, duration and whether the cloud coverage is provided across different network zones.	X	X	X
Routine Costs	Marketing and PR Costs	Marketing and PR costs are used to communicate new implementations that are made by the providers from whom the company obtains its supplies. This is a cost borne entirely by the company and we classify it as a short-term "investment". These costs are higher depending on the occurrence of the event and its size. However, they are low compared to the others.	X	X	X
Non-routine Costs	Incident Response Costs	This cost depends directly on the number of experts and consultants that are hired to understand the causes of the cloud outage. It is also proportional to the size of the event and therefore to the number of outages and the duration.	X	X	X

Modelling Methodology

The modelling part of the cloud outage scenario consists of mapping the magnitude and type of an attack into shocks to the different voices on a company's balance sheet. Each of the three case study companies modelled is generically associated with the real market and the sector to which it belongs. We tried to reproduce a cloud outage on the basis of qualitative and quantitative characteristics typical of the sector.

Cash Flow Impacts

Risk Reduction by Scenario, Case Study Company, and Control. shows the impact of a cloud outage on the balance sheet of the companies under consideration.

Modelling Overview

The cloud outage model is based on the following key drivers:

- The number of outages that occurred in the time horizon considered
- The duration of the event
- The percentage of business/portion of region/s where the outage occurs
- The adopted cloud outage services and their regional coverage

These parameters provide a measure of the shock to the balance sheets of the companies chosen as case studies. The technical characteristics of the

Table 23: EV@Risk Results – Cloud Outage (Source: CCRS Analysis).

Case Study Company	EV@Risk 5yr, \$ millions (L1 to L4 Losses)	EV@Risk % Loss	Weighted Average Expected Loss 5 yr, \$ millions	Weight Average Expected % Loss
Transportation	\$3.14 to \$199.18	0.05% to 3.2%	\$9.15	0.15%
Apparel Retail	\$44.44 to \$885.23	0.12% to 2.30%	\$29.61	0.08%
Manufacturing	\$4.82 to \$1265.97	0.02% to 5.34%	\$28.19	0.12%

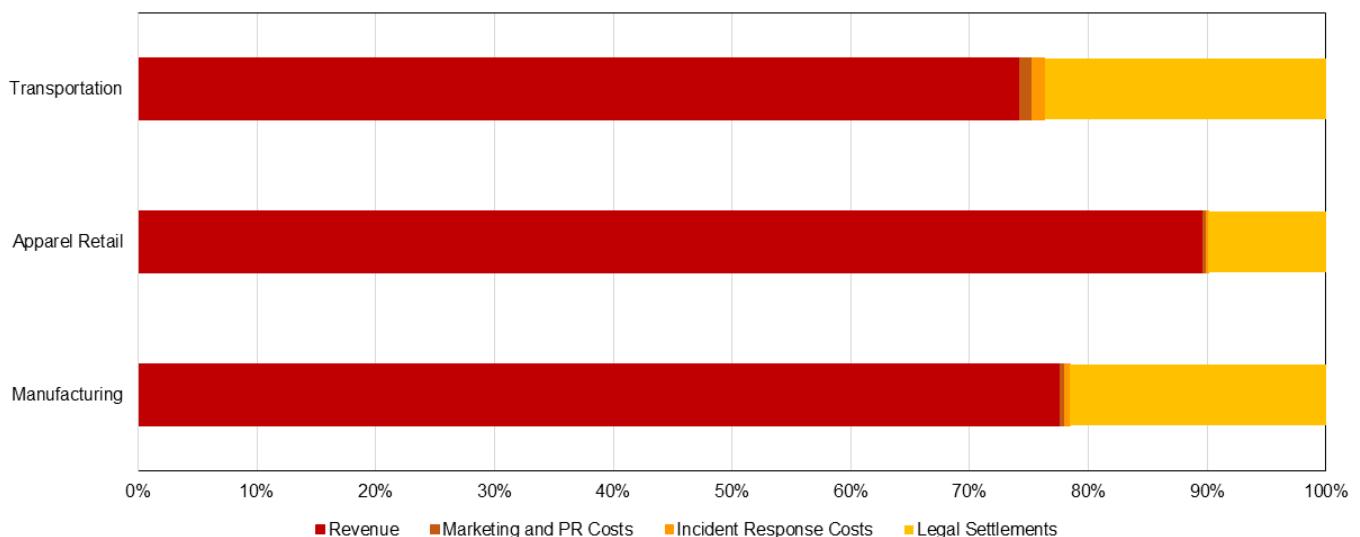


Figure 19: Decomposition of 5 year EV@Risk Results by Cash Flow Category for Cloud Outage Scenario for L2 (Source: CCRS Analysis).

disruption (number of outages, duration etc.) directly influence the impact on revenues (e.g., through the business interruption). The portion of the disrupted business defines the severity of the four levels of the scenario (L1-L4).

To characterise the size of the cloud outage, we used proxies for the shares of the impacted regions of the companies. The logic is to associate the impacted regions with the business interruption and consequently with the deriving shocks. This also indicates some diversity within the pool of selected companies (depending on industry characteristics).

Incident response costs also depends in some measures on the number of outages and their duration.

The other two cash flow impacts represented by marketing and PR costs and legal and settlement costs are modelled through the qualitative assumptions of experts.

Full details on the cloud outage scenario can be found in the Appendix section ‘Modelling Methodology’.

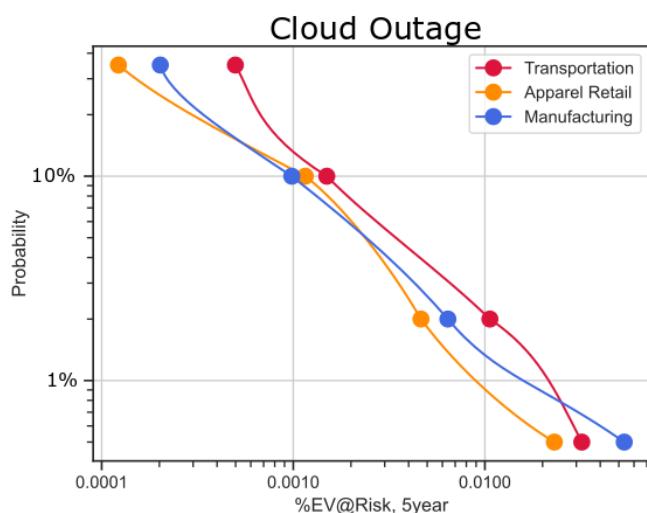


Figure 20: Cloud Outage Impact Overview by Level and Case Study Company (Source: CCRS Analysis).

Scenario Loss Results

The following table summarises the scenario modelling results. The first column shows the total financial impact of the scenario for L1 to L4 levels modelled. The middle column shows the % of the EV baseline each of those L1 to L4 level results in the left column represent. Finally, the last column shows the weighted average expected EV@Risk over the next 5 years, meaning it is the multiplication of the EV@ Risk and probability for each level modelled and then the weighted average of all levels modelled.

Table 24: Cloud Outage Risk Reduction Results (Source: CCRS Analysis).

Control	Transportation	Apparel Retail	Manufacturing
Control 19	8 to 32%	9 to 17%	9 to 34%

The primary cash flow category of loss is revenue while legal settlements is the secondary category driving the losses for the Cloud Outage scenario.

Risk Mitigation Results

We also report the corresponding results in terms of absolute risk mitigation for each company in Risk Reduction by Scenario, Case Study Company, and Control..

Conclusions

The aim of this section is to provide some tools for interpreting an extremely technical and complex event such as a cloud outage from an economic point of view. We have performed this through the case studies of three companies belonging to three different sectors (transportation, retail, and manufacturing sectors). We proposed an approach based on the territorial coverage offered by six major cloud service providers. We translated the technical drivers (number of outages per region and duration) into economic shocks. Finally, we concluded with a perspective on the possible mitigation actions that companies can implement to reduce risk. Our research concludes that control 19 is the only effective and directly implementable strategy for companies to mitigate risk.

8 Summary of Results and Conclusions

The loss modelling research by scenario showed that different cash flow categories are driving the losses by scenario as shown in Risk Reduction by Scenario, Case Study Company, and Control. for the L2 level modelled. Revenue is the primary driver of loss in all the L2 levels modelled. It might be surprising to see Revenue impacts as the primary driver for Data Breach scenarios, but in all the levels modelled it is assumed that corporates experience some disruption to their IT services as their security teams take systems offline in an effort to reduce the spread of the attack. This table changes drastically for the more extreme variants and when looking at specific companies as the results presented in the previous chapter show. For example, in the Data Breach scenario for the L4 level and for the Transportation company, the primary driver is Compensation Costs, the secondary driver being Legal Settlements and Revenue is only seen as the tertiary loss driver.

Table 25: Summary of Loss Drivers by Scenario for the L2 Level Only.

Loss Driver	Ransom-ware	Data Breach	Cloud Outage
Primary	Revenue	Revenue	Revenue
Secondary	Ransom Payment	Legal Settlements	Legal Settlements
Tertiary	Legal Settlements	Compensation Costs	Incident Response Costs

Table 26 summarises the weighted average expected 5-year EV@Risk for each scenario and each cash study company, both in millions USD and in percent loss share. The Manufacturing company is most impacted (% loss) by the ransomware driven by the direct impact to their production processes from the malware with a gradual return to full capacity. While for Transportation and Apparel Retail companies Data Breach is the most impactful (% loss) scenario. Looking across the rows of scenarios, the Transportation company sees the biggest loss percent for the Data Breach and Cloud Outage Scenarios, with Manufacturing experiencing the largest percent loss for the Ransomware event.

Looking at the total risk exposure results in comparison to the BitSight ratings, the Manufacturing Company should be performing the worst overall, but its revenue dependency on cloud services and the amount of sensitive consumer data held are both much lower in comparison to the other sectors represented. The losses faced by the Transportation company are in line with the low BitSight rating. The Apparel Retail company suffers the smallest exposure matching its high BitSight Rating.

The data breach is of great significance to the transport and apparel retail companies as they handle a lot of customer data. This increases the impact on compensation costs and revenues especially in the most extreme scenarios. Since the manufacturing company only engages business with other companies, the customer pool (the key driver of the size of the data breach) is limited and so is the final impact from the model.

The cloud outage is a lower impact event than the other two mainly because the more extreme scenarios are associated with low probabilities while the lower impact scenarios are characterised by short durations and a limited number of occurring events. This is in line with the description given in the previous sections: extreme cloud outages are very rare, and responsibilities and costs are to be verified and are shared between users and providers.

The following table summarises the EV@Risk for each level prior to multiplying by probability to get the expected loss, shown in the above table. This is a helpful metric to show us just how big an event can be with losses in the \$1 to 2 billion range. Scenario losses range from 8 to 18 percent of earning value (EV) for the ransomware scenario, from 1 to 16 percent of EV for the Data Breach scenario and from 2 to 5 percent for the most extreme level (L4).

Risk Reduction Observations

Turning to look at risk reduction, Figure 21 shows a visual of the maximum outcome from implementing better malware defences (Control 8) at the Transportation company for the Ransomware scenario. Here we can see that the implementation reduced the likelihood and the cost of the event for all the levels modelled. Further, this reduction brought the tail of the loss distribution closer to the risk tolerance line. Figure 22 shows all subplots for all the case study companies, all three scenarios and

Table 26: Weighted Average Expected Loss 5-year by Scenario (Source: CCRS Analysis).

Scenario	Transportation		Apparel Retail		Manufacturing	
	\$ millions	% Loss	\$ millions	% Loss	\$ millions	% Loss
Ransomware	\$42.01	0.68%	\$174.86	0.23%	\$87.32	0.74%
Data Breach	\$88.91	1.43%	\$187.63	0.79%	\$33.38	0.14%
Cloud Outage	\$9.15	0.15%	\$29.61	0.08%	\$28.19	0.12%
Total Risk Exposure	\$140.07	2.25%	\$392.10	1.02%	\$148.89	0.63%
BitSight Rating	640		790		620	

Table 27: Summary of EV@Risk by Level by Scenario (Source: CCRS Analysis).

Case Study Company	Ransomware	Data Breach	Cloud Outage
EV@Risk, \$ millions			
Transportation	\$7.24 to \$1,162.66	\$25.8 to \$998.1	\$3.14 to \$199.18
Apparel Retail	\$22.95 to \$2,969.71	\$73.6 to \$1,979.6	\$44.44 to \$885.23
Manufacturing	\$27.26 to \$2,532.25	\$18.96 to \$227.38	\$4.82 to \$1265.97
EV@Risk, % Loss			
Transportation	0.12% to 18.70%	0.41% to 16.05%	0.05% to 3.2%
Apparel Retail	0.06% to 7.73%	0.31% to 8.34%	0.12% to 2.30%
Manufacturing	0.11% to 10.67%	0.08% to 0.96%	0.02% to 5.34%

all 4 controls modelled. Charts focused on a single control are included in the Appendix and numeric results are summarised in Table 27

The cyber security controls modelling highlights some interesting results. The Transportation Company sees the largest risk reduction by improving their malware defences (Control 8) for both the Ransomware and Data Breach Scenarios. While for the Apparel Retail Company configuration management (Control 5) gives the biggest return for Ransomware, and we see a tie between malware defences and configuration management in terms of returns for the Data Breach Scenario. Finally, the Manufacturing Company sees the greatest gain from Control 5 for the Ransomware scenario and Control 8 for the Data Breach scenario. For Cloud Outage, only one control was modelled, yet it is insightful to see potential gains for just improving the company's incident response plan (Control 19).

Qualitatively, the best combination of controls to implement against Ransomware appears to be

Controls 5 and 8. It reduces both the exposure to risk and the likelihood of occurrence by combining the implementation of anti-malware systems and control systems that reduce misconfigurations.¹

These controls are equally effective against Data Breach with the only difference that, for Manufacturing, Control 19 is more effective than Control 5 due to the potential for Incident Response Plans to reduce duration of disruption to production systems. In addition, Control 8 for Manufacturing is the most efficient and its implementation would be able to reduce the risk of even the most severe scenario (L4) to an acceptable level.

Regarding the risk of Cloud Outage, Control 19 (the only control considered for mitigation) is particularly effective for Transportation and Manufacturing. In the first case, severity levels for scenarios L2, L3 and L4

¹ Please note combinations of controls was not studied in this report.

are reduced to the point where they no longer represent an impactful risk (given the company's characteristics). In the second case, there is a shift from a red area (above risk tolerance) to a yellow area (major concern) for L4 while L2 becomes a controlled risk.

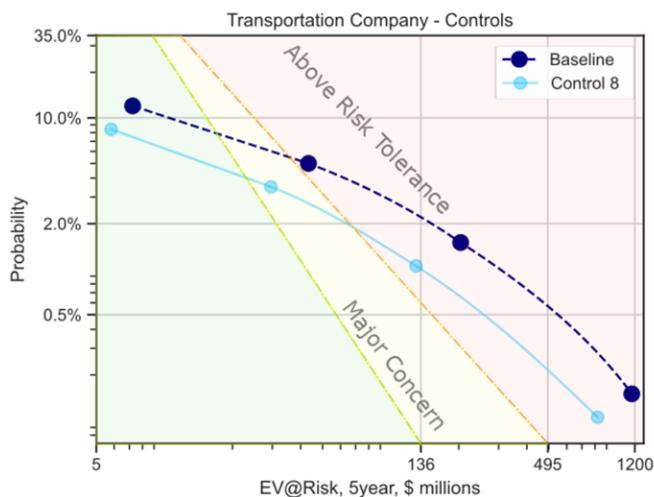


Figure 21: Maximum Impact of Control 8 in Reducing Ransomware Risk for a Transportation Company (Source: CCRS Analysis).

Conclusions

The model presented represents a framework which empowers a wide range of corporates to quantify the impacts from three cyber scenarios on their cash flows, looking at losses in multiple categories of cash flow without focusing on one representation of the risk impact.

The results provide reliable comparative numbers

to emphasise the qualitative instinct that different industries have different risk exposures. Manufacturing is heavily exposed to the Ransomware scenario, while Transportation and Apparel Retail are more exposed to the Data Breach Scenario.

Notably, this framework is expanded to quantify the potential risk reduction from implementation of control improvements. This is novel among reports of this type and means that organisations can use this framework to examine the risk/reward trade-offs of implementing specific controls solutions. More specifically, this framework could be used to determine return on investment (ROI) from specific control improvements. Control 19, focusing on improvements to incident response plans and strategy, highlights that even organisational changes can have decent gains in risk reduction at very little upfront investment by an organisation.

Establishing a controls baseline against industry peers was helpful in quantifying the potential room for improvement in cyber mitigations and contingency planning. Corporates should establish a controls baseline as a first step to embarking on a risk reduction quantification exercise as outlined in this report.

Finally, more research, measurement and telemetry work will be required to improve the parameterisation of the risk reduction potential. There are several key academic findings on patching cadence and risk reduction (Control 3), but there is far less work thus far on the other controls modelled. IT Service Providers website suggest extreme risk reduction particularly for anti-malware but should be challenged and refined with more robust and unbiased data capture.

Table 28: Comparison of Controls Risk Reduction by Scenario and by Case Study Company (Source: CCRS Analysis).

Control	Transportation	Apparel Retail	Manufacturing
Ransomware			
Control 3	6 to 47%	4 to 34%	9 to 22%
Control 5	3 to 47%	6 to 48%	7 to 51%
Control 8	11 to 52%	5 to 43%	10 to 49%
Control 19	4 to 27%	4 to 19%	6 to 27%
Data Breach			
Control 3	8 to 15%	11 to 39%	4 to 10%
Control 5	6 to 55%	9 to 49%	4 to 14%
Control 8	16 to 56%	12 to 49%	12 to 44%
Control 19	3 to 17%	5 to 14%	4 to 22%
Cloud Outage			
Control 3	-	-	-
Control 5	-	-	-
Control 8	-	-	-
Control 19	8 to 31%	8 to 17%	9 to 34%

9 References

- Abrams, Lawrence. 2021. “Microsoft April 2021 Patch Tuesday Fixes 108 Flaws, 5 Zero-Days.” Bleeping Computer. April 13, 2021. <https://www.bleepingcomputer.com/news/microsoft/microsoft-april-2021-patch-tuesday-fixes-108-flaws-5-zero-days/>.
- Ahmad, Atif, Kevin C. Desouza, Sean B. Maynard, Humza Naseer, and Richard L. Baskerville. 2020. “How Integration of Cyber Security Management and Incident Response Enables Organizational Learning.” *Journal of the Association for Information Science and Technology* 71 (8): 939–53. <https://doi.org/10.1002/asi.24311>.
- AICPA. n.d. “SOC for Service Organizations.” Accessed December 6, 2021. <https://us.aicpa.org/interestareas/frc/assuranceadvisoryservices/socforserviceorganizations>.
- Allodi, Luca. 2015. “The Heavy Tails of Vulnerability Exploitation.” In *Engineering Secure Software and Systems*, edited by Frank Piessens, Juan Caballero, and Natalia Bielova, 133–48. Lecture Notes in Computer Science. Cham: Springer International Publishing. https://doi.org/10.1007/978-3-319-15618-7_11.
- Arikan, Burak. 2017. “Analyzing the NPM Dependency Network.” *Graph Commons* (blog). October 17, 2017. <https://medium.com/graph-commons/analyzing-the-npm-dependency-network-e2cf318c1dod>.
- Aviat Networks. 2020. “8-K Press Release Exhibits Q2FY20 PRE.” SEC.Gov. January 22, 2020. <https://www.sec.gov/Archives/edgar/data/1377789/000137778920000002/a8-kpressreleaseexhibitsq2.htm>.
- Bailey, Tucker, James Kaplan, and Allen Weinberg. 2012. “Playing War Games to Prepare for a Cyberattack,” no. 26: 6.
- BBC News. 2010. “Shell Employee Details Revealed,” February 12, 2010. <http://news.bbc.co.uk/1/hi/business/8512390.stm>.
- . 2018. “Air Canada App Data Breach Involves Passport Numbers,” August 29, 2018, sec. Technology. <https://www.bbc.com/news/technology-45349056>.
- . 2020a. “Cathay Pacific Fined £500,000 over Customer Data Protection Failure,” March 4, 2020, sec. Technology. <https://www.bbc.com/news/technology-51736857>.
- . 2020b. “Marriott Hotels Fined £18.4m for Data Breach That Hit Millions,” October 30, 2020, sec. Technology. <https://www.bbc.com/news/technology-54748843>.
- BitSight Technologies. 2021a. “BitSight: Security Ratings Leader - Cyber Risk Management Solutions.” BitSight. 2021. <https://www.bitsight.com>.
- . 2021b. “Ransomware: The Rapidly Evolving Trend.” BitSight. 2021. <https://info.bitsight.com/ransomware-the-rapidly-evolving-trend>.
- Browne, Ryan, and Sam L Shead. 2021. “What Is Fastly and Why Did It Just Take a Bunch of Major Websites Offline?” CNBC. June 8, 2021. <https://www.cnbc.com/2021/06/08/fastly-outage-internet-what-happened.html>.
- Busby, Joshua W., Kyri Baker, Morgan D. Bazilian, Alex Q. Gilbert, Emily Grubert, Varun Rai, Joshua D. Rhodes, Sarang Shidore, Caitlin A. Smith, and Michael E. Webber. 2021. “Cascading Risks: Understanding the 2021 Winter Blackout in Texas.” *Energy Research & Social Science* 77 (July): 102106. <https://doi.org/10.1016/j.erss.2021.102106>.
- Cadet, Carlo. 2021. “Evidence-Based Strategies for Ransomware Prevention.” BitSight. May 20, 2021. <https://www.bitsight.com/blog/ransomware-prevention>.
- CIS. 2019. “CIS Critical Security Controls v7.1.” CIS. 2019. <https://www.cisecurity.org/controls/v7/>.
- . 2020. “Controls Version 8.” CIS. May 2020. <https://www.cisecurity.org/controls/v8/>.
- Clayton, Chairman Jay. 2018. “Statement on Cybersecurity Interpretive Guidance.” SEC. Gov. February 21, 2018. <https://www.sec.gov/news/public-statement/statement-clayton-2018-02-21>.
- CloudSecurityAlliance. 2020. “Consensus Assessment Initiative Questionnaire (CAIQ) v3.1.” CSA. April 1, 2020. <https://cloudsecurityalliance.org/artifacts/consensus-assessments-initiative-questionnaire-v3-1/>.
- Concinnity Risks. 2021. “RansomCoin DB.” 2021. <https://billing.concinnity-risks.com/>.
- Constantin, Lucian. 2019. “Macy’s Breach Is a Game-

- Changing Magecart Attack | CSO Online.” December 19, 2019. <https://www.csoonline.com/article/3510643/macys-breach-is-a-game-changing-magecart-attack.html>.
- Costello, Katie, and Meghan Rimol. 2021. “Gartner Forecasts Worldwide Public Cloud End-User Spending to Grow 23% in 2021.” Gartner. April 21, 2021. <https://www.gartner.com/en/newsroom/press-releases/2021-04-21-gartner-forecasts-worldwide-public-cloud-end-user-spending-to-grow-23-percent-in-2021>.
- De Groot, Juliana. 2020. “Biggest Manufacturing Data Breaches of the 21st Century.” Text. Digital Guardian. August 7, 2020. <https://digitalguardian.com/blog/biggest-manufacturing-data-breaches-of-the-21st-century>.
- Diffblue. 2019. “Developer Survey.”
- Duffy, Clare. 2021. “A Massive Ransomware Attack Hit Hundreds of Businesses. Here’s What We Know.” CNN. July 7, 2021. <https://www.cnn.com/2021/07/06/tech/kaseya-ransomware-what-we-know/index.html>.
- EasyJet Claim. 2020. “EasyJet Data Breach Compensation Claim | PGMBM.” EasyJet Data Breach | PGMBM Law. 2020. <https://theeasyjetclaim.com/>.
- ENow Software. 2021. “Office 365 Monitoring: Teams Outage (June 11, 2021).” June 12, 2021. <https://www.enowsoftware.com/office-365-monitoring-outages/microsoft-teams-outage-june-11-2021>.
- Eurostat. 2021. “Cloud Computing - Statistics on the Use by Enterprises.” 2021. https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Cloud_computing_-_statistics_on_the_use_by_enterprises.
- Farrer, Martin. 2021. “Airline Data Hack: Hundreds of Thousands of Star Alliance Passengers’ Details Stolen.” *The Guardian*, March 2021, sec. World news. <https://www.theguardian.com/world/2021/mar/05/airline-data-hack-hundreds-of-thousands-of-star-alliance-passengers-details-stolen>.
- FIRST. 2021. “The EPSS Model.” FIRST — Forum of Incident Response and Security Teams. 2021. <https://www.first.org/epss/model>.
- Foley, Mary Jo. 2020a. “Microsoft’s March 3 Azure East US Outage: What Went Wrong (or Right)?” ZDNet. March 6, 2020. <https://www.zdnet.com/article/microsofts-march-3-azure-east-us-outage-what-went-wrong-or-right/>.
- . 2020b. “GitHub Hit with Multiple Back-to-Back Outages.” ZDNet. April 23, 2020. <https://www.zdnet.com/article/github-hit-with-multiple-back-to-back-outages/>.
- . 2020c. “Microsoft’s Azure AD Authentication Outage: What Went Wrong.” ZDNet. October 1, 2020. <https://www.zdnet.com/article/microsofts-azure-ad-authentication-outage-what-went-wrong/>.
- Fruhlinger, Josh. 2020. “The CIA Triad: Definition, Components and Examples.” CSO Online. February 10, 2020. <https://www.csoonline.com/article/3519908/the-cia-triad-definition-components-and-examples.html>.
- Goldman, David. 2021. “Verizon Fios Customers Report Outages across the East Coast - CNN.” January 26, 2021. <https://edition.cnn.com/2021/01/26/tech/verizon-fios-outage/index.html>.
- Google, Google Dashboard. 2021. “Google Cloud Status Dashboard.” November 2021. <https://status.cloud.google.com/incidents/6PM5mNd43NbMqjCZ5REh>.
- Graham-Cumming, John. 2020. “Cloudflare Outage on July 17, 2020.” The Cloudflare Blog. July 18, 2020. <http://blog.cloudflare.com/cloudflare-outage-on-july-17-2020/>.
- Greenberg, Andy. 2021. “Beyond Kaseya: Everyday IT Tools Can Offer ‘God Mode’ for Hackers.” *Wired*, July 12, 2021.
- Greig, Jonathan. 2020. “Study Finds Misconfigured Cloud Storage Services in 93% of Cloud Deployments Analyzed.” TechRepublic. August 4, 2020. <https://www.techrepublic.com/article/study-finds-misconfigured-cloud-storage-services-in-93-of-cloud-deployments-analyzed/>.
- Hiscox. 2021. “The Hiscox Cyber Readiness Report 2021 | Hiscox UK.” 2021. <https://www.hiscox.co.uk/cyberreadiness>.
- Householder, Allen D, Jeff Chrabaszcz, Trent Novelly, and David Warren. n.d. “Historical Analysis of Exploit Availability Timelines,” 9.
- ISO. n.d. “ISO - ISO/IEC 27001 — Information Security Management.” ISO. Accessed December 6, 2021. <https://www.iso.org/isoiec-27001-information-security.html>.
- Jacobs, Jay, Sasha Romanosky, Idris Adjerid, and Wade Baker. 2020. “Improving Vulnerability Remediation through Better Exploit Prediction.” *Journal of Cybersecurity* 6 (1): tyaa015. <https://doi.org/10.1080/24709860.2020.1734420>.

- doi.org/10.1093/cybsec/tyaa015.
- Jacobs, Jay, Sasha Romanosky, Benjamin Edwards, Idris Adjerid, and Michael Roytman. 2021. “Exploit Prediction Scoring System (EPSS).” *Digital Threats: Research and Practice* 2 (3): 1–17. <https://doi.org/10.1145/3436242>.
- Janardhan, Santosh. 2021. “Update about the October 4th Outage.” *Engineering at Meta* (blog). October 5, 2021. <https://engineering.fb.com/2021/10/04/networking-traffic/outage/>.
- Kassner, Michael. n.d. “Anatomy of the Target Data Breach: Missed Opportunities and Lessons Learned.” ZDNet. Accessed November 30, 2021. <https://www.zdnet.com/article/anatomy-of-the-target-data-breach-missed-opportunities-and-lessons-learned/>.
- Kentik. 2021. “Facebook Suffers Global Outage.” Kentik. October 4, 2021. <https://www.kentik.com/analysis/facebook-suffers-global-outage/>.
- Kirk, Jeremy. 2016. “Aircraft Part Manufacturer Says Cybercrime Incident Cost It \$54 Million.” CSO Online. January 22, 2016. <https://www.csionline.com/article/3025401/aircraft-part-manufacturer-says-cybercrime-incident-cost-it-54-million.html>.
- Kivu. 2020. “Successful Ransomware Is Organized Crime (TLP:White).” Kivu (blog). 2020. <https://kivuconsulting.com/download/successful-ransomware-is-organized-crime-2/>.
- Kivu, and Hiscox. 2020. “New Report Combines Kivu and Hiscox Data on Ransomware Trends.” Kivu (blog). 2020. <https://kivuconsulting.com/resources/new-report-combines-kivu-and-hiscox-data-on-ransomware-trends/>.
- Knight, Richard, and Jason R. C. Nurse. 2020. “A Framework for Effective Corporate Communication after Cyber Security Incidents.” *Computers & Security* 99 (December): 102036. <https://doi.org/10.1016/j.cose.2020.102036>.
- Krutchén, Philippe, Robert Nord, and İpek Ozkaya. 2012. “Technical Debt: From Metaphor to Theory and Practice.” *IEEE Software* 26 (2). <https://doi.org/10.1109/MS.2012.167>.
- LaCroix, Kevin. 2021a. “Title Insurance Company Settles SEC Cybersecurity Disclosure-Related Charges.” The D&O Diary. June 16, 2021. <https://www.dandodiary.com/2021/06/articles/securities-laws/title-insurance-company-settles-sec-cybersecurity-disclosure-related-charges/>.
- . 2021b. “SEC Charges Company Over Misleading Cybersecurity-Related Disclosures.” The D&O Diary. August 17, 2021. <https://www.dandodiary.com/2021/08/articles/cyber-liability/sec-charges-company-over-misleading-cybersecurity-related-disclosures/>.
- Leverett, É, Matilda Rhode, and Adam Wedgbury. 2020. “Vulnerability Forecasting: In Theory and Practice.” *ArXiv*.
- Lévesque, Fanny Lalonde, Sonia Chiasson, Anil Somayaji, and José M. Fernandez. 2018. “Technological and Human Factors of Malware Attacks: A Computer Security Clinical Trial Approach.” *ACM Transactions on Privacy and Security* 21 (4): 18:1–18:30. <https://doi.org/10.1145/3210311>.
- Lourerio, Sergio. 2020. “What Are Security Misconfigurations and How to Prevent Them? | Outpost 24 Blog.” Outpost24. June 30, 2020. <https://outpost24.com/blog/What-are-security-misconfigurations-and-how-to-prevent-them>.
- MacAfee. 2014. “How Bad Is the eBay Breach? Here Are the Stats | McAfee Blogs.” May 22, 2014. <https://www.mcafee.com/blogs/enterprise/cloud-security/how-bad-is-the-ebay-breach-here-are-the-stats/>.
- Madory, Doug. 2021. “Facebook’s Historic Outage, Explained.” Kentik Blog. October 5, 2021. <https://www.kentik.com/blog/facebook-s-historic-outage-explained/>.
- Maimon, David. 2019. “Existing Evidence for the Effectiveness of Antivirus in Preventing Cyber Crime Incidents,” 3.
- MITRE. 2020. “Mitigations - Enterprise | MITRE ATT&CK®.” 2020. <https://attack.mitre.org/mitigations/enterprise/>.
- Nakasone, Paul. 2021. *TESTIMONY ON UNITED STATES SPECIAL OPERATIONS COMMAND AND UNITED STATES CYBER COMMAND IN REVIEW OF THE DEFENSE AUTHORIZATION REQUEST FOR FISCAL YEAR 2022 AND THE FUTURE YEARS DEFENSE PROGRAM*.
- Narcisi, Gina. 2021a. “Verizon Outage Hits East Coast As Users Begin Work.” CRN. March 3, 2021. <https://www.crn.com/news/networking/verizon-outage-hits-east-coast-as-users-begin-work>.
- . 2021b. “Akamai Outage Takes Down Global Banks, Airline Websites.” CRN. June 17, 2021. <https://www.crn.com/news/networking/akamai-outage-takes-down-global-banks>.

airline-websites.

National Cyber Security Centre. n.d. "About Cyber Essentials." Accessed December 6, 2021. <https://www.ncsc.gov.uk/cyberessentials/overview>.

National Vulnerability Database. 2021. "NVD - Statistics." 2021. <https://nvd.nist.gov/products/cpe/statistics>.

Nichols, Shaun. 2020. "Yes, It's down Again: Microsoft's Office 365 Takes yet Another Mid-Week Tumble, Azure Also Unwell." October 7, 2020. https://www.theregister.com/2020/10/07/office_365_outage/.

NIST. 2021. "NIST RMF Quick Start Guide - Implement Step - FAQs." March 2021. <https://csrc.nist.gov/CSRC/media/Projects/risk-management/documents/04-Implement%20Step/NIST%20RMF%20Implement%20Step-FAQs.pdf>.

NIST Joint Task Force. 2020. "Security and Privacy Controls for Information Systems and Organizations." NIST Special Publication (SP) 800-53 Rev. 5. National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.SP.800-53r5>.

Olcott, Jake. 2021. "Colonial Pipeline Is Not Alone: Ransomware Risk in the U.S. Oil/Energy Sector." BitSight. May 17, 2021. <https://www.bitsight.com/blog/colonial-pipeline>.

O'Neill, Ashley, Atif Ahmad, and Sean Maynard. 2021. "Cybersecurity Incident Response in Organisations: A Meta-Level Framework for Scenario-Based Training." *ArXiv:2108.04996 [Cs]*, August. <http://arxiv.org/abs/2108.04996>.

Osborne, Charlie. n.d. "Oil Giant Shell Discloses Data Breach Linked to Accellion FTA Vulnerability." ZDNet. Accessed November 30, 2021. <https://www.zdnet.com/article/oil-giant-shell-discloses-data-breach-linked-to-accellion-fta-vulnerability/>.

Palmer, Danny. 2019. "Ransomware: The Key Lesson Maersk Learned from Battling the NotPetya Attack." ZDNet. April 29, 2019. <https://www.zdnet.com/article/ransomware-the-key-lesson-maersk-learned-from-battling-the-notpetya-attack/>.

—. n.d. "Ransomware: New File-Encrypting Attack Has Links to GandCrab Malware, Say Security Researchers." ZDNet. Accessed November 30, 2021. <https://www.zdnet.com/article/ransomware-new-file-encrypting-attack-has-links-to-gandcrab-malware-say-security->

researchers/.

Porter, Jon. 2021. "Google Docs and Sheets Experienced a Partial Outage." The Verge. April 12, 2021. <https://www.theverge.com/2021/4/12/22379701/google-docs-down-drive-sheets-slides-outage-classroom>.

Ramel, By David, and 04/13/2020. 2020. "Microsoft Confirms March Azure Outage Due to COVID-19 Strains -." Visual Studio Magazine. April 13, 2020. <https://visualstudiomagazine.com/articles/2020/04/13/azure-outage.aspx>.

Reuters. 2021. "British Airways Settles with 2018 Data Breach Victims | Reuters." July 6, 2021. <https://www.reuters.com/business/aerospace-defense/british-airways-reaches-settlement-with-customers-over-2018-data-breach-2021-07-06/>.

Risk Based Security. 2021. "2020 Year End Data Breach QuickView Report." 2021. <https://pages.riskbasedsecurity.com/en/en/2020-yearend-data-breach-quickview-report>.

SAP. 2020. "2020 SAP Integrated Report." SEC.Gov. 2020. https://www.sec.gov/Archives/edgar/data/0001000184/000110465921034734/tm218829d1_ex99-1.htm.

SEC. 2018. "Commission Statement and Guidance on Public Company Cybersecurity Disclosures," February, 24.

SEC.gov. 2018a. "SEC Adopts Statement and Interpretive Guidance on Public Company Cybersecurity Disclosures." February 21, 2018. <https://www.sec.gov/news/press-release/2018-22>.

—. 2018b. "SEC Investigative Report: Public Companies Should Consider Cyber Threats When Implementing Internal Accounting Controls." October 16, 2018. <https://www.sec.gov/news/press-release/2018-236>.

—. 2021a. "SEC Charges Issuer With Cybersecurity Disclosure Controls Failures." June 15, 2021. <https://www.sec.gov/news/press-release/2021-102>.

—. 2021b. "SEC Charges Pearson Plc for Misleading Investors About Cyber Breach." August 16, 2021. <https://www.sec.gov/news/press-release/2021-154>.

—. 2021c. "EDGAR Application Programming Interfaces." September 28, 2021. <https://www.sec.gov/edgar/sec-api-documentation>.

Security Scorecard. 2015. "U.S. Military Manufacturer Experiences Data Breach | SecurityScorecard."

- July 5, 2015. <https://securityscorecard.com/blog/u-s-military-manufacturer-experiences-data-breach>.
- Sharwood, Simon, and APAC Editor. 2020. “From Off-Prem to Just off: IBM Cloud Goes down Planet-Wide so Hard Even the Status Page Didn’t Work.” June 9, 2020. https://www.theregister.com/2020/06/09/ibm_cloud_outage/.
- Shead, Sam. 2021. “Reddit and Global News Sites Including FT, New York Times and Bloomberg Experience Outage.” CNBC. June 8, 2021. <https://www.cnbc.com/2021/06/08/reddit-and-global-news-sites-go-offline.html>.
- Sonatype. 2020. “2020 Software Supply Chain Report | Download.” Sonatype. August 12, 2020. <https://www.sonatype.com/resources/white-paper-state-of-the-software-supply-chain-2020>.
- Statista. 2021. “Percent of Corporate Data Stored in the Cloud 2021.” Statista. 2021. <https://www.statista.com/statistics/1062879/worldwide-cloud-storage-of-corporate-data/>.
- Stempel, Jonathan. 2020. “Home Depot Reaches \$17.5 Million Settlement over 2014 Data Breach.” Reuters, November 24, 2020, sec. U.S. Legal News. <https://www.reuters.com/article/us-home-depot-cyber-settlement-idUSKBN2842W5>.
- Stevens, Melissa. 2016. “Analyzing 3 Major Data Breaches Of 2015.” April 5, 2016. <https://www.bitsight.com/blog/analyzing-major-data-breaches-2015>.
- Sudhakar, and Sushil Kumar. 2020. “An Emerging Threat Fileless Malware: A Survey and Research Challenges.” *Cybersecurity* 3 (1): 1. <https://doi.org/10.1186/s42400-019-0043-x>.
- Tsidulko, Joseph. 2020. “Salesforce Instance Failure Causing Widespread Service Disruption.” CRN. August 11, 2020. <https://www.crn.com/news/cloud/salesforce-instance-failure-causing-widespread-service-disruption>.
- Verizon. 2020. “2020 DBIR Summary of Findings | Verizon Enterprise Solutions.” 2020. <https://www.verizon.com/business/resources/reports/dbir/2020/summary-of-findings/>.
- . 2021. “2021 Data Breach Investigations Report.” Verizon Business. 2021. <https://www.verizon.com/business/resources/reports/dbir/>.
- Vincent, James. 2020. “Zoom Is Working Again, Even If You’re Not.” The Verge. August 24, 2020. <https://www.theverge.com/2020/8/24/21398900>
- zoom-down-outages-us-uk-meetings-webinars.
- Warren, Tom. 2021. “Microsoft Teams, Exchange and More Went down for Four Hours on Monday.” The Verge. March 15, 2021. <https://www.theverge.com/2021/3/15/22332539/microsoft-teams-down-outage-connectivity-issues>.
- Zelivansky, Ariel, and Yuval Avrahami. 2021. “What You Need to Know About Azurescape.” *Palo Alto Networks Blog* (blog). September 9, 2021. <https://www.paloaltonetworks.com/blog/2021/09/azurescape/>.

Appendix

In this appendix, we provide several additional views of the modelled results.

Ransomware Decomposition Figures

The following figures show the decomposition of modelled results by cash flow category for each case study company for the Ransomware scenario.

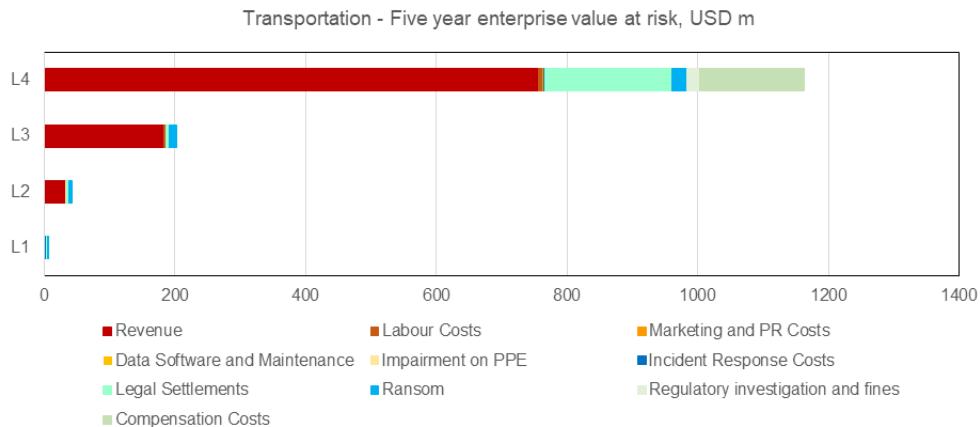


Figure 22: Ransomware Loss Decomposition – Transportation (Source: CCRS Analysis).

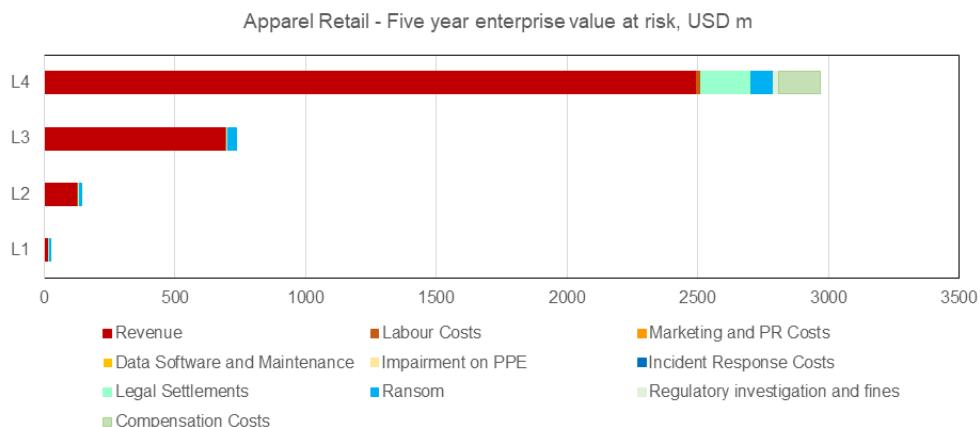


Figure 23: Ransomware Loss Decomposition – Apparel Retail (Source: CCRS Analysis).

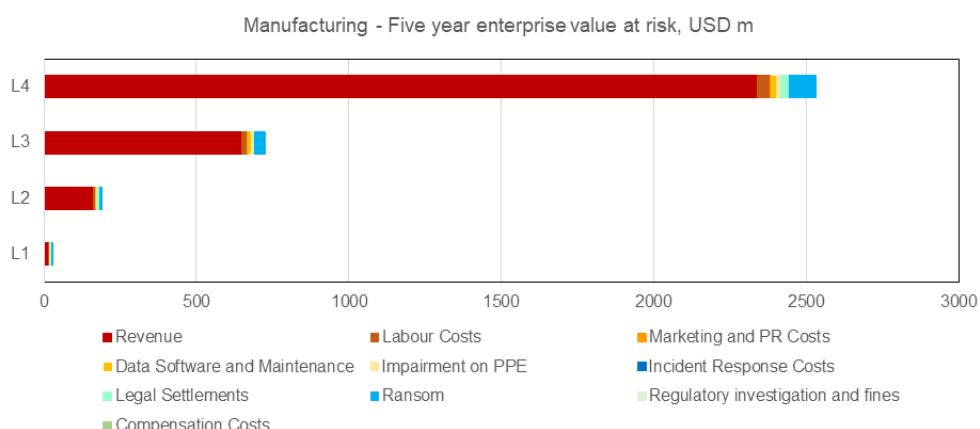


Figure 24: Ransomware Loss Decomposition – Manufacturing (Source: CCRS Analysis).

Data Breach Decomposition Figures

The following figures show the decomposition of modelled results by cash flow category for each case study company for the Data Breach scenario.

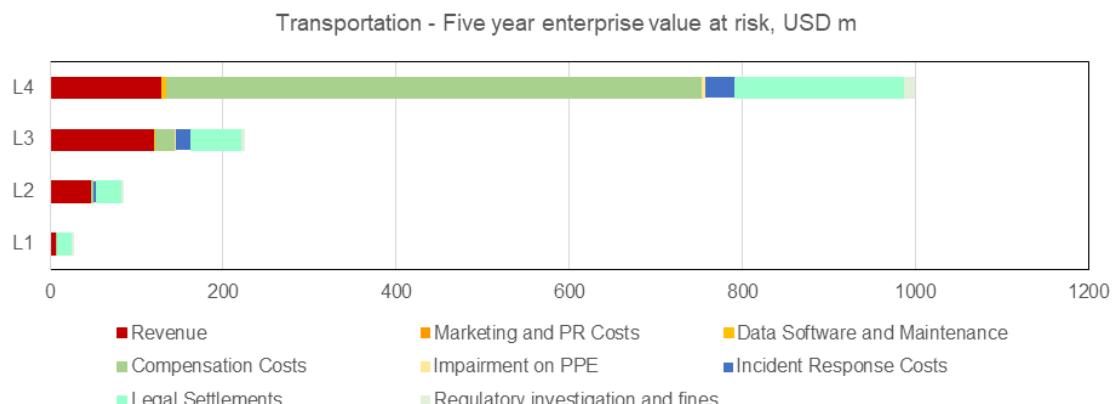


Figure 25: Data Breach Loss Decomposition – Transportation (Source: CCRS Analysis).

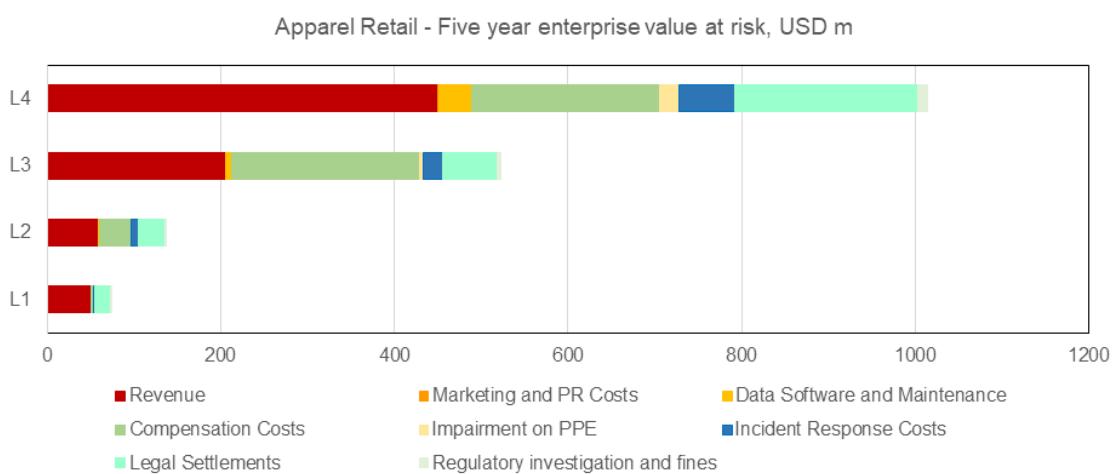


Figure 26: Data Breach Loss Decomposition – Apparel Retail (Source: CCRS Analysis).

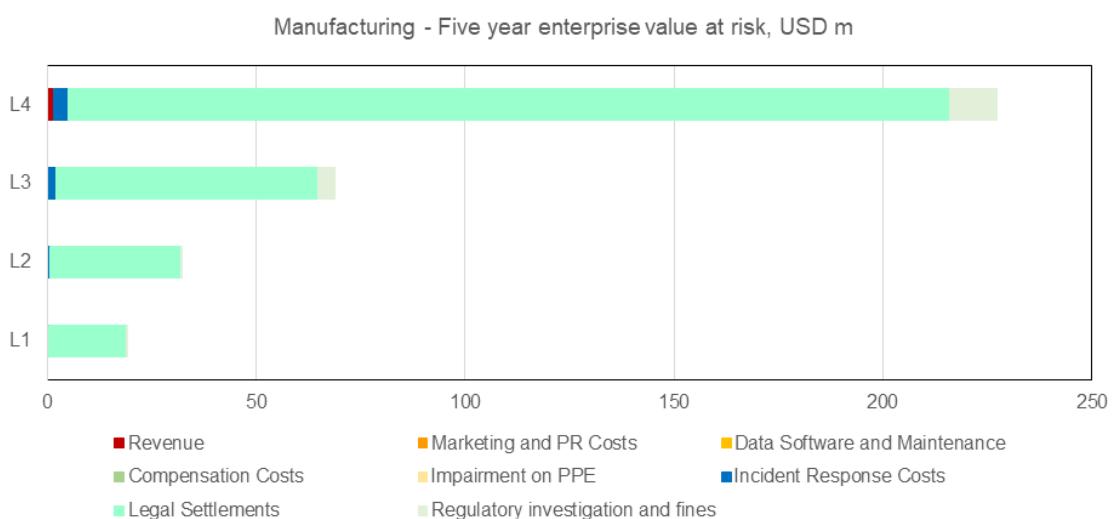


Figure 27: Data Breach Loss Decomposition – Manufacturing (Source: CCRS Analysis).

Cloud Outage Decomposition Figures

The following figures show the decomposition of modelled results by cash flow category for each case study company for the Cloud Outage scenario.

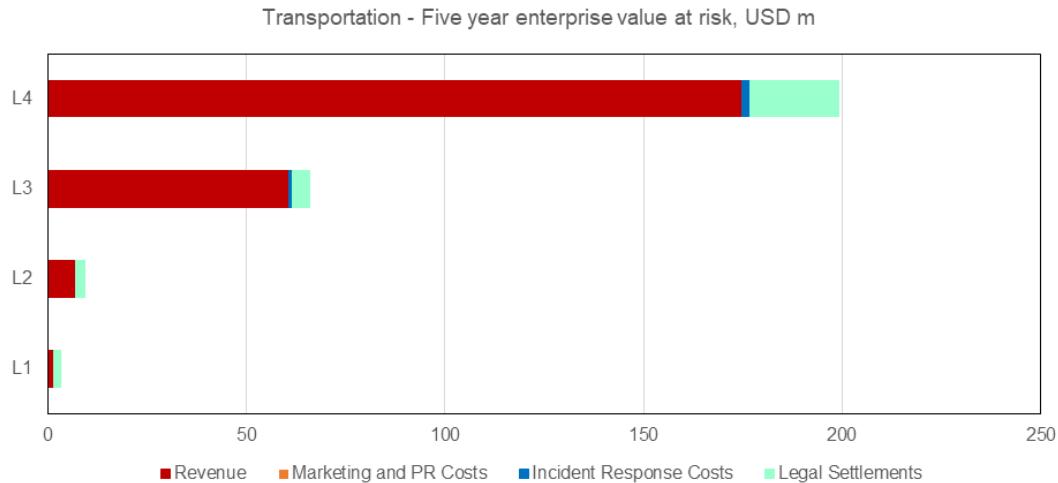


Figure 28: Cloud Outage Decomposition – Transportation (Source: CCRS Analysis).

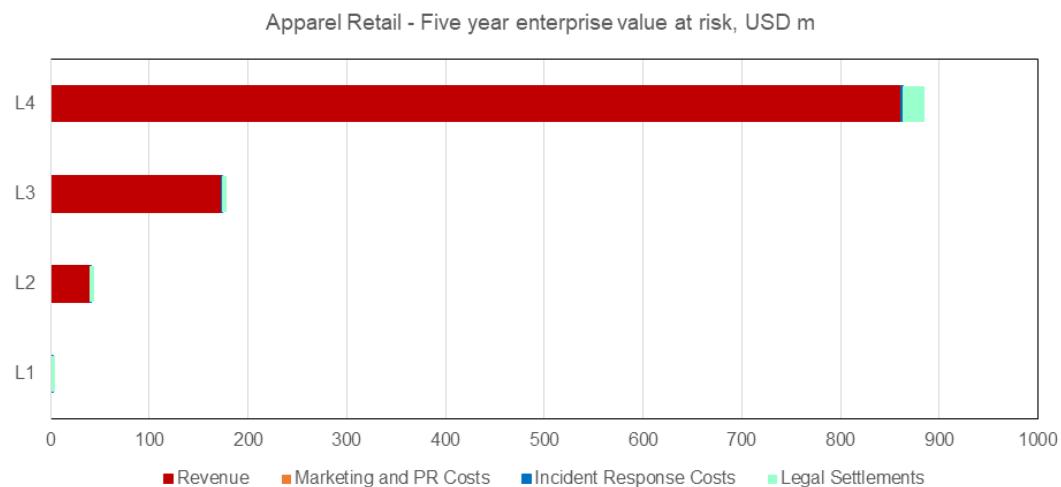


Figure 29: Cloud Outage Decomposition – Apparel Retail (Source: CCRS Analysis).

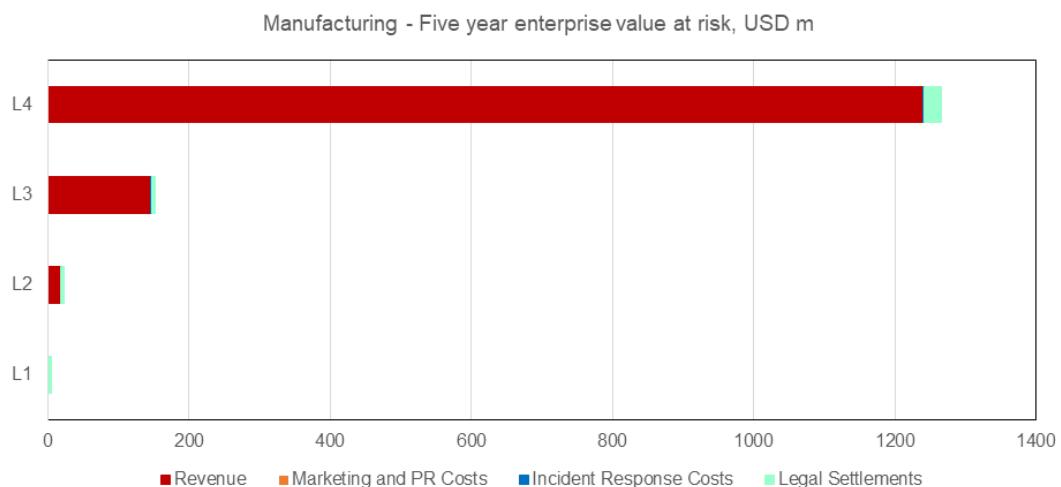


Figure 30: Cloud Outage Decomposition – Manufacturing (Source: CCRS Analysis).

EV@Risk Grouped by Scenario

Figure 31 shows the baseline summary EV@Risk results for each case study company and all three scenarios in one plot.

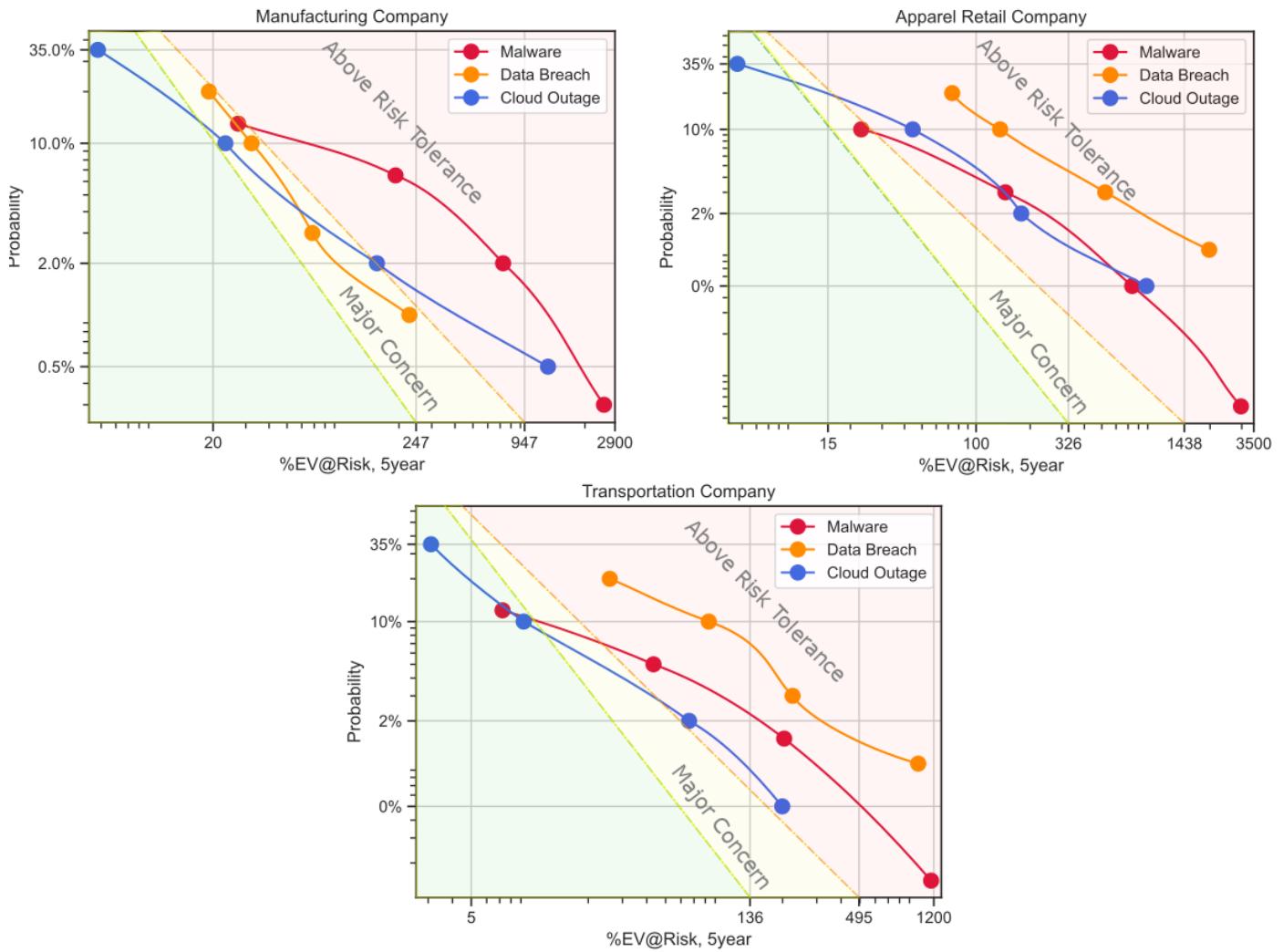


Figure 31: Summary of Scenario Losses, Baseline, for all case study companies.

Further Controls Charts

This section has further subplot charts showing each control reduction per scenario and per case study company.

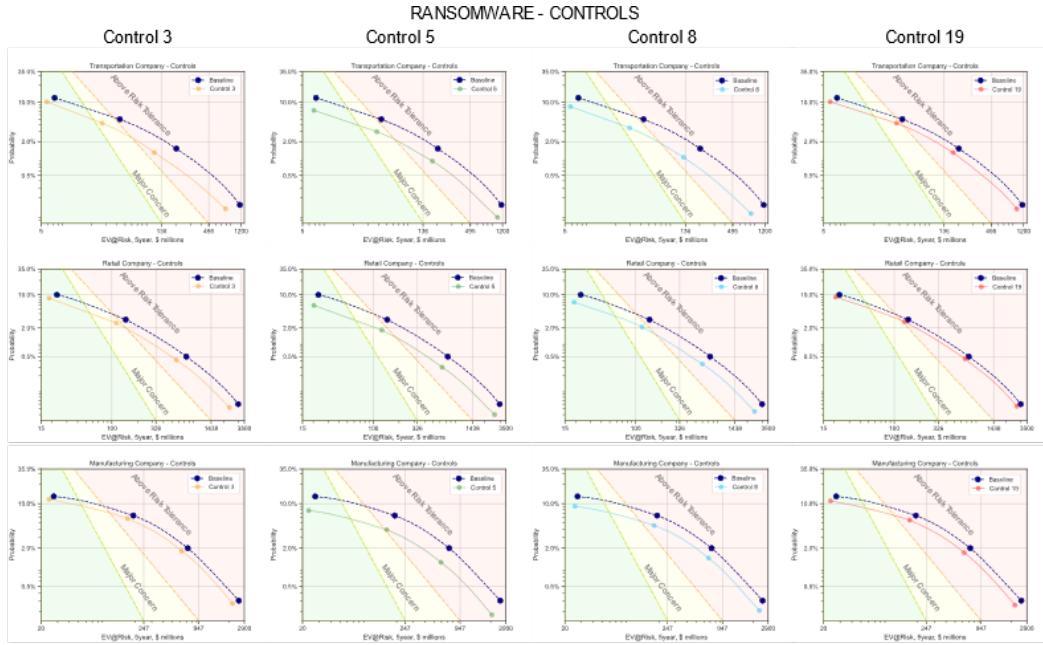


Figure 32: Ransomware Scenario Risk Reduction by Case Study Company and Control.

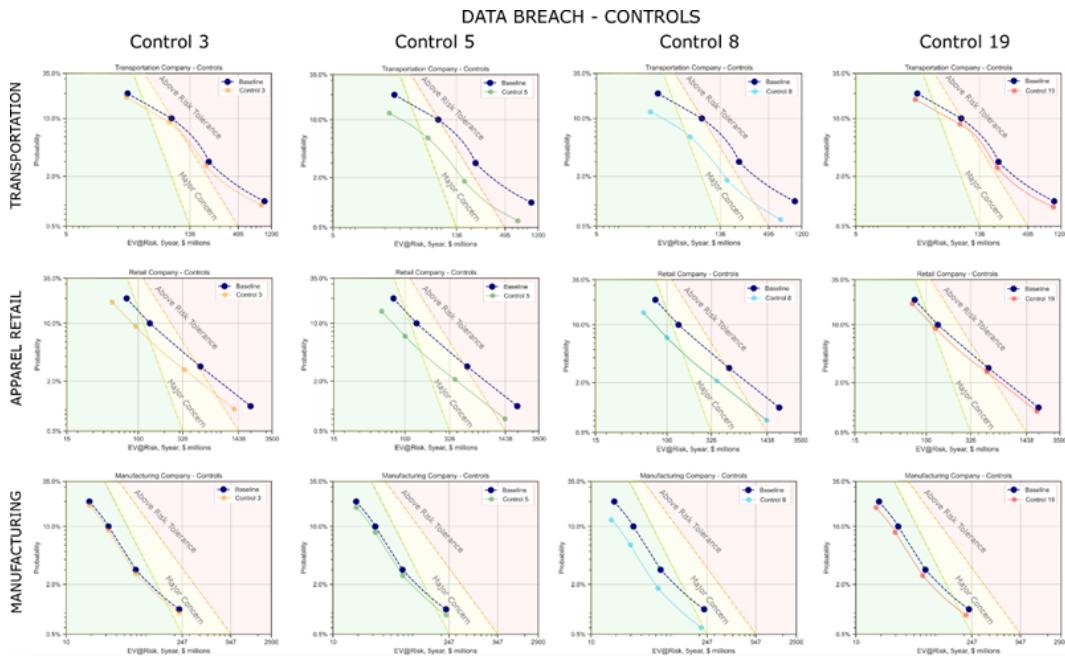


Figure 33: Data Breach Scenario Risk Reduction by Case Study Company and Control.

CLOUD OUTAGE - CONTROLS

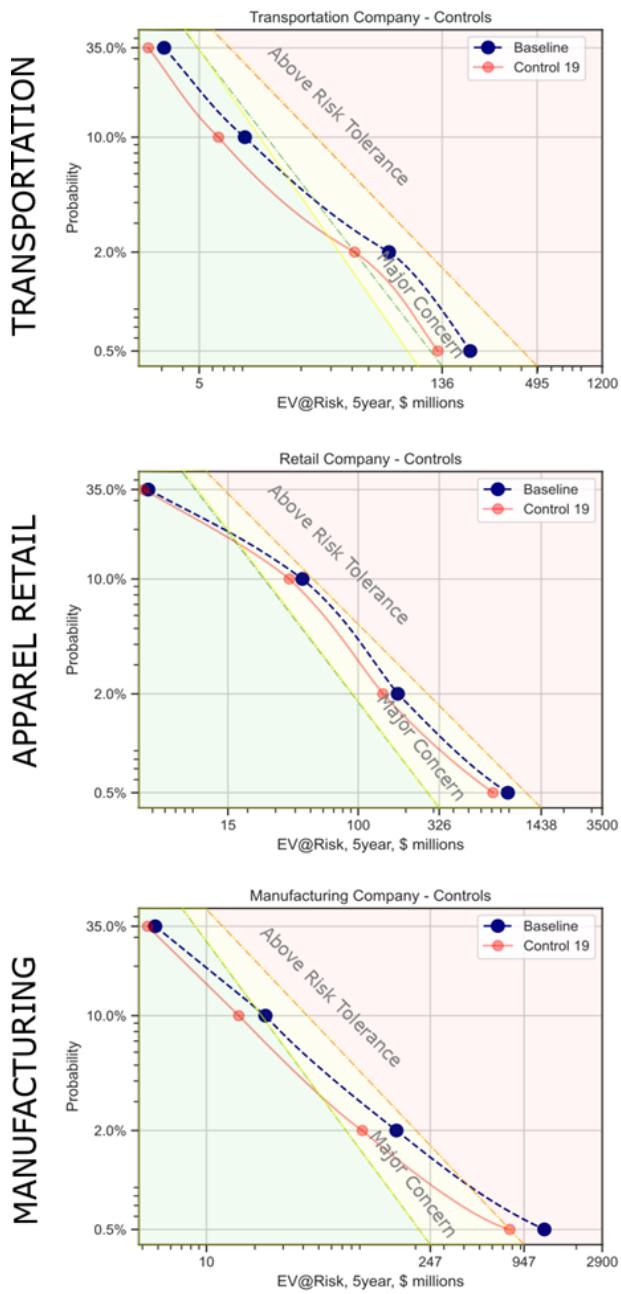


Figure 34: Cloud Outage Scenario Risk Reduction by Case Study Company and Control.

This report is based on original research by the Cambridge Centre for Risk Studies at the University of Cambridge Judge Business School.

The following people contributed the research, model development, and writing of this report.

Cambridge Centre for Risk Studies

Dr Jennifer Daffron, Project Lead and Research Associate
Jennifer Copic, Cyber Model Lead and Senior Risk Researcher
Gabriele La Malfa, Risk Researcher
Dr Jay Jung, Senior Risk Researcher
Kiran Sridhar, Risk Researcher
Matteo Ilardo, Risk Researcher
Dr Andrew Coburn, Chief Scientist
Tamara Evan, Report Editor and Risk Researcher

BitSight

Stephen Boyer, Founder and Chief Technology Officer
Jake Olcott, VP Communications and Government Affairs
Tom Montroy, Director of Data Science
Andrew Burton, Director, Thought Leadership Content
Ethan Geil, Senior Director of Data and Research
Matt Cherian, VP, Security Performance Management
Lydia Dwyer, Cybersecurity Senior Product Manager

The Cambridge Centre for Risk Studies greatly appreciates the valuable guidance and support of the following individuals in the making of this report:

Winston Krone, Chief Research Officer at Kivu Consulting
Eireann Leverett, Founder and CEO at Concinnity Risks
Erin Burns, Co-Founder and Director of Offensive Research at Concinnity Risks
Dr Eric Jardine, Affiliate at Concinnity Risks and Assistant Professor of Political Science at Virginia Tech

Cambridge Centre for Risk Studies

Cambridge Judge Business School
University of Cambridge
Trumpington Street
Cambridge
CB2 1AG

T: +44 (0) 1223 768386

F: +44 (0) 1223 339701

enquiries.risk@jbs.cam.ac.uk

www.risk.jbs.cam.ac.uk

Join our LinkedIn group at Cambridge
Centre for Risk Studies

Follow us @Risk_Cambridge