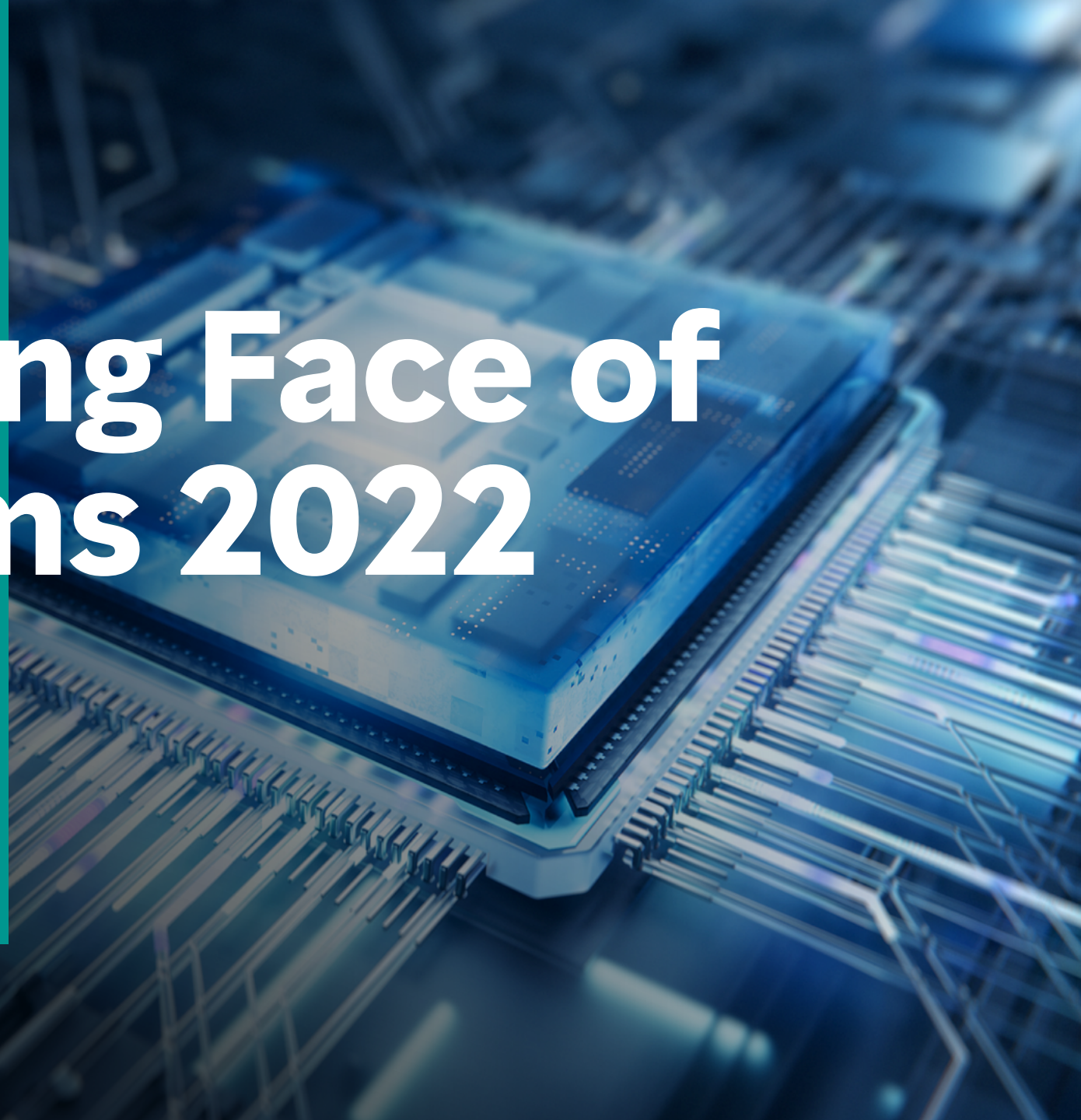
Marsh

The Changing Face of Cyber Claims 2022

A cyber insurance loss study
in continental Europe



October 2022

Contents

Introduction Page 3

1 Cyber claims continue to rise Page 4

2 Manufacturing sees a surge in cyber claims Page 8

3 Cyber hygiene can help minimise cyber incidents Page 13

4 Supply chain attacks on the rise Page 16

Conclusion Page 18

Introduction

The increasing sophistication and evolution of cyber threat actors and their methods continues to drive the number of cyberattacks higher. As attacks increase, so do related cyber insurance claims.

In **The Changing Face of Cyber Claims 2022**, Marsh looks at trends and changes in cyber claims in the region through the end of 2021, as well as some of the steps organisations can take to mitigate their impact.

Not surprisingly, the number of claims reported by clients increased from 2020 to 2021. Interestingly, the proportion of claims based on malicious events versus accidental ones also increased.

We also found the manufacturing sector to be subject, for the first time, to more total claims than any other sector when looking at cumulative totals from 2016 through 2021.

The report also examines the vulnerabilities in supply chains, which are too often overlooked by organisations yet can leave them vulnerable to attack.

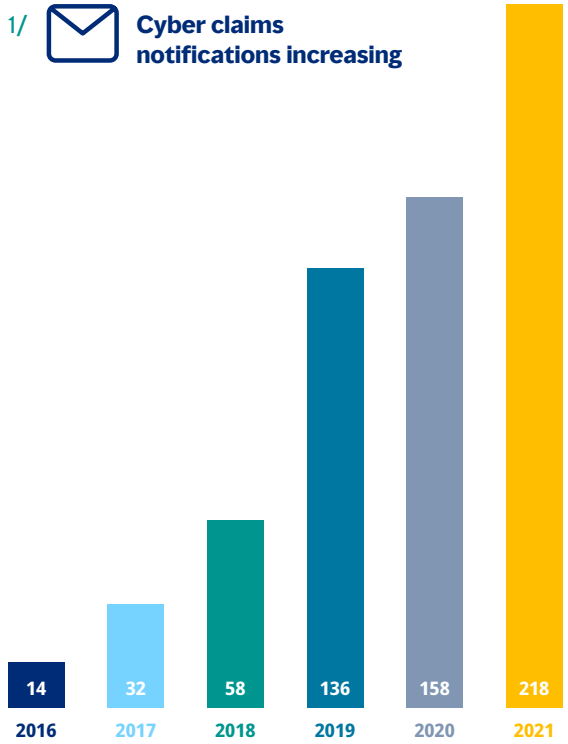
Whether it's protecting the supply chain or mitigating cyber risks in other parts of the organisation, many companies are improving their cyber hygiene by implementing some or all of 12 key controls. Insurers are also paying attention to these controls, and are asking for information regarding their use during underwriting.

Cyber claims continue to rise

The number of cyber insurance policies Marsh placed across Europe continued to grow between 2020 and 2021 but was outstripped by the number of cyber claims which grew by 37% year on year *(see Figure 1)*.

As underwriters scrutinised submissions, clients generally took higher retentions, changed sub-limits, and focused on insurance strategy.

1/ **Cyber claims notifications increasing**

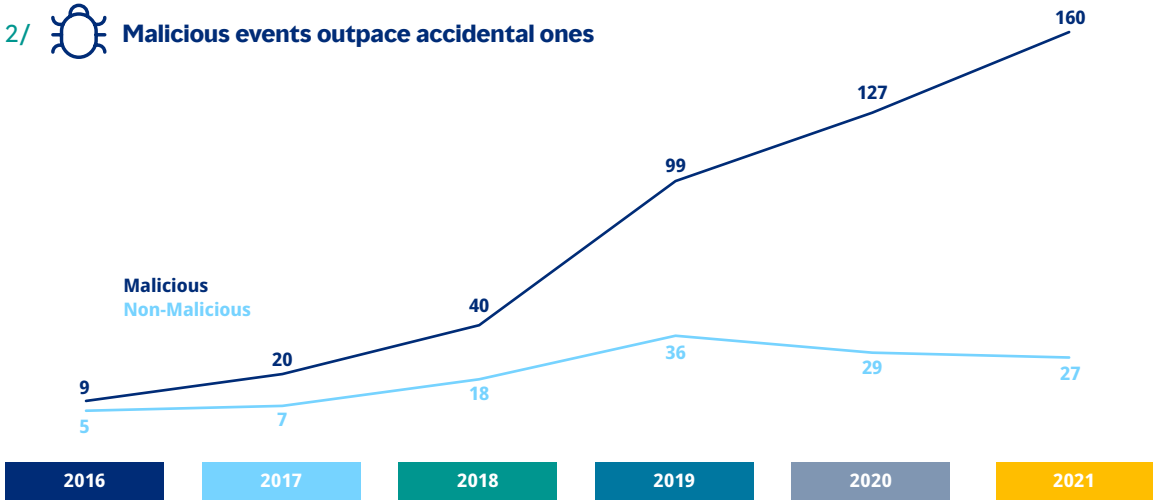


The number of malicious events continued to increase while non-malicious, or “accidental”, events decreased *(see Figure 2)*.

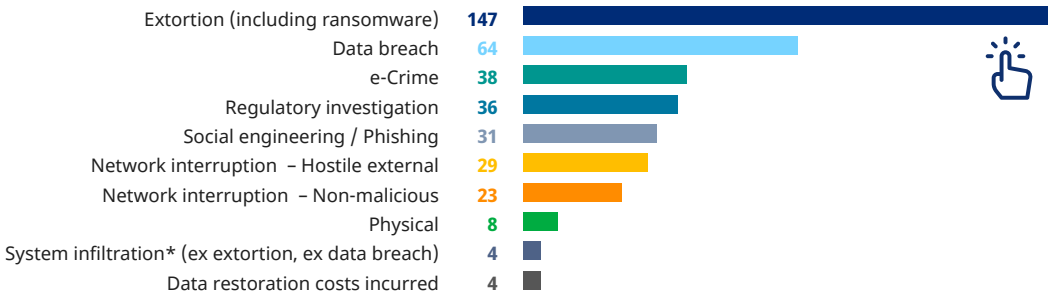
In **2019**, the ratio of malicious to non-malicious events was 73:27; by **2021** the ratio had increased to 86:14. The **decrease in accidental** events comes as companies deploy more effective cyber controls, including employee training. The **increase in malicious** events was driven largely by the ability of threat actors to evolve and develop increasingly sophisticated techniques.

Among the incidents analysed, extortion events — including ransomware — were the largest share at 38%. This number is larger than the following three leading causes combined, those being data breaches, 17%; e-crime, 10%, and regulatory investigations, 9%. Social engineering is the 5th most frequent incident at 8% *(see Figure 3, mouse over the graph to see the definition of these terms)*.

2/ Malicious events outpace accidental ones



3/ Extortion, including ransomware, is the most common claim incident



Definition of different types of cyber crime

Extortion:
Whenever software related to known cases of ransomware is identified or a ransom payment is demanded for the recovery of data, unblocking systems, or stopping leaks of data.

Data breach:
When sensitive data has been unlawfully accessed through diverse means by external parties (brute access to network, trojans, and so forth) or where sensitive data has been leaked by accident (email with wrong addressees, improper disposal of files, and so forth).

e-Crime:
Cases of impersonation or identify fraud such as the so-called "fake president", as well as transmission interception, fraud wired payments, and so forth.

Regulatory investigation:
Where regulatory breaches have occured such as GDPR incompliance, where personal data has been shared with third parties without previous approval and so forth.

Social engineering/ Phishing:
Any cases of identified phishing attempts.

Network interruption – hostile external:
A company's systems are encrypted or down through denial-of-service attack (DDOS) attacks where no ransom demand has been received.

Network interruption – non-malicious:
The company's system cannot operate due to a fault such as a software update.

Physical:
Physical damage to hardware/equipment and theft of physical equipment.

System infiltration:
An unauthorised access to the network has been identified, but no data has been compromised and no demand has taken place. Usually because the attempt is shut down in time.

Data restoration:
Due to human error, data is overwritten, corrupted, or deleted.

Globally, there are signs that progress is being made in battling the ransomware epidemic.

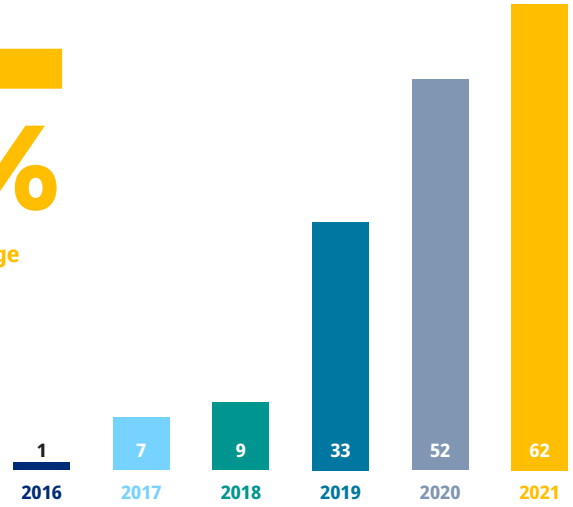
As noted by Coveware, the number of companies paying ransoms to resolve an incident has trended lower over a recent 12 quarter span. Additionally, they note a **34% decrease** in the average ransom payment from the fourth quarter of 2021 to the second quarter of 2022.

However, continued diligence with regard to controls will be required in order to maintain progress, which, in turn, should improve cyber underwriting results.

4/ Ransomware claims continue to increase

34%

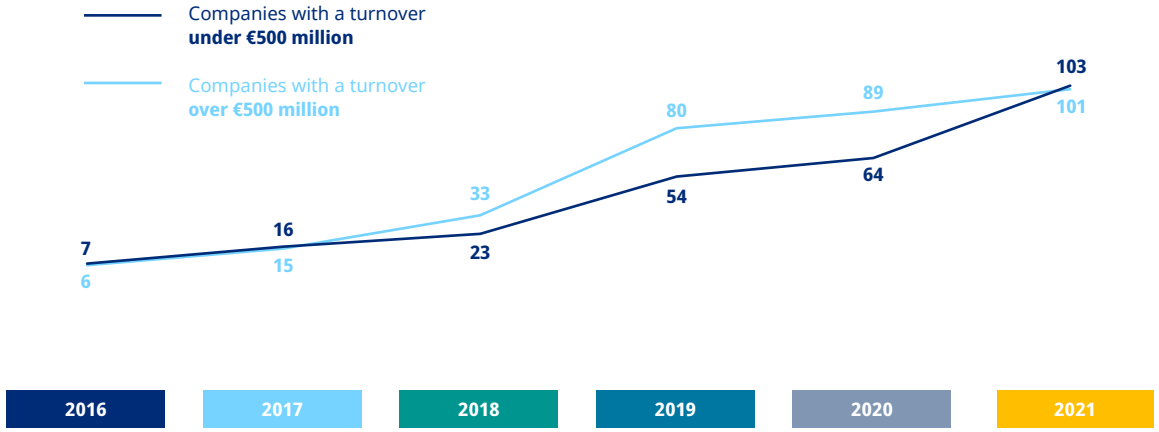
decrease in average ransom payment from Q4 2021 and Q2 2022



The frequency of cyber incidents for companies with a turnover greater than €500 million increased at a slower rate than for those with a turnover less than €500 million, likely driven by larger companies' ability to invest more in cybersecurity and resilience *(see Figure 5)*.

Between 2019 and 2021 claims for companies with a turnover of under €500 million increased by 90% during the same period companies with a turnover of over €500 million grew by 26%.

5/ Frequency of cyber claims higher for smaller companies



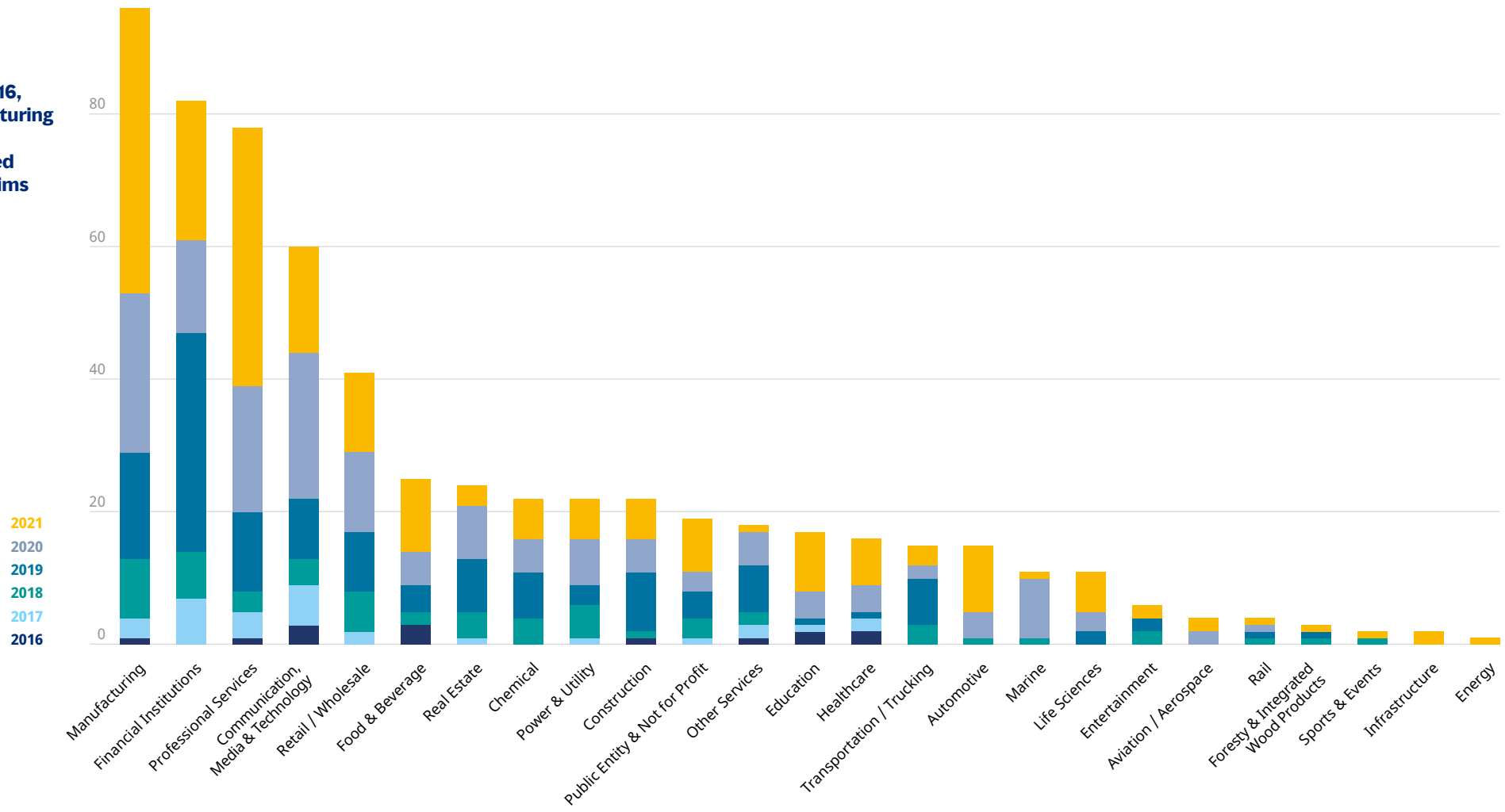
Manufacturing sees a surge in cyber claims

Cumulatively since 2016, the manufacturing industry has filed the highest number of claims notifications, surpassing the financial institutions sector in 2021 *(see Figure 6)*. This may reflect higher investments in cyber resilience within the financial sector, such as staff training and basic cyber hygiene. The financial services and healthcare sectors have developed regulatory frameworks for third-party risk testing, and have standards that vendors need to comply with, for example, the Payment Card Data Security Standards (PCI-DSS), which dictates levels of software quality and mobile payment components.

At the same time, cyberattacks have increased against the manufacturing industry, which has been relatively late implementing defence mechanisms. Manufacturers also typically have lower maturity in operational technology (OT) and industrial control systems (ICS), while their dependence on systems and automation has grown rapidly.

6/

Since 2016, manufacturing sector submitted most claims



The **manufacturing sector** was not alone in seeing a rise in their cyber claims in 2021; there were also large rises in the number of claims in the professional services sector, the food and beverage industry, the education sector, and in the automotive sector.

The **manufacturing sector** has seen a dramatic rise in the number of cyber claims over the last five years, having grown from three in 2017 to 43 in 2021. The jump in the number of claims between 2020 and 2021, while not the highest leap in percentage terms, was the largest rise in number of incidents seen in the sector, almost doubling from 23 in 2020 to 43 in 2021.

378%

The number of claims from the manufacturing sector in Marsh's portfolio skyrocketed from 9 in 2019 by **378%** to 43 in 2021.

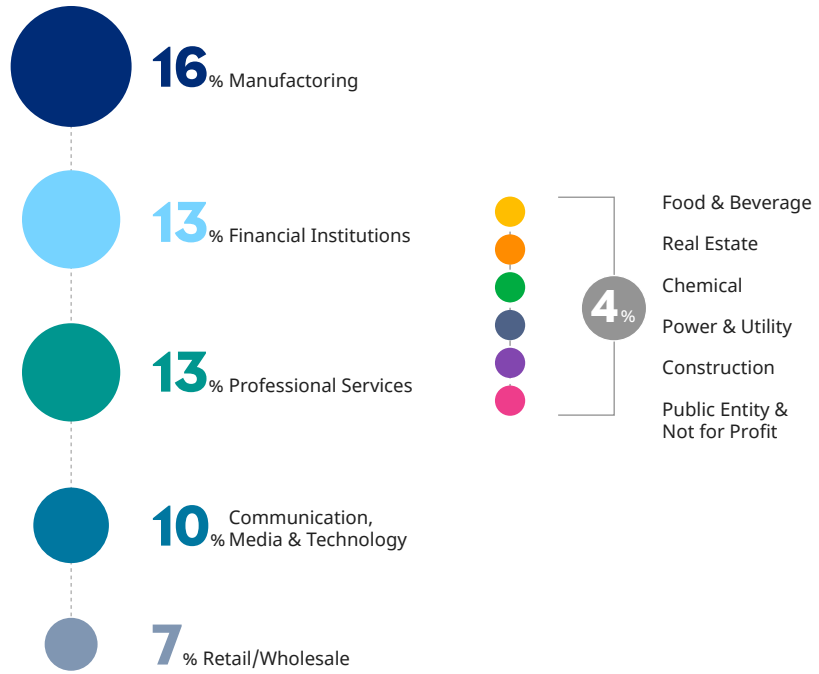
91%

An astonishing 91% of the cyber incidents in the manufacturing sector are classified as malicious, even higher than the industry average of 86%.

As companies continue their transition towards digitalisation and industry 4.0, a term that refers to increasing digital processes within firms, integrating those processes within smart value chains, and enabling new cyber-physical technologies such as internet of things enabled devices and mechanisms, the area of attack for threat actors grows. The benefits for embracing this process outweigh the negative implications but those negative implications still exist and every attempt to mitigate them must be made by the firms who could experience them. The manufacturing sector, in particular, is moving towards both digitalisation and industry 4.0 at speed and must embrace heightened security minded measures with the same enthusiasm.

Implementation of new technologies within the manufacturing sector often means onboarding new partners within the digital supply chain of an organisation. This can be both on the software and hardware sides of things as well as any programmes or systems that help integrate new technology with existing parts of a company's operations. Every time a new partner is added to the digital supply chain it is another door that can allow a threat actor in. Ensuring those possible avenues remain closed and maintaining high levels of digital hygiene all along the supply chain becomes an increasingly important task for an organisation.

7/ **Claims by industry between 2016 and 2021**



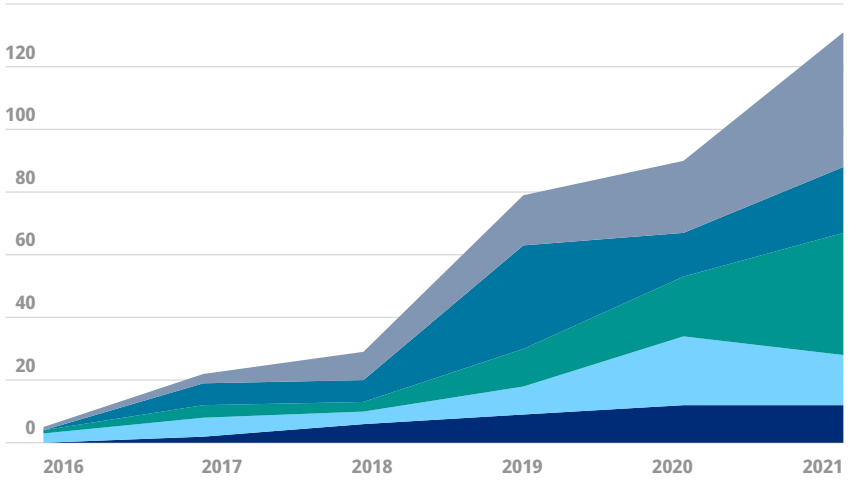
Marsh data showed that ransomware was the leading cause of cyber incidents, with three times as many events attributed to it as the second highest cause, network interruption.

While the number of incidents is on the rise in the **manufacturing sector**, the average loss of each incident is declining, falling from just under €1.9 million in 2019 to just over **€1 million in 2021**. One key factor in this trend is the ability of companies and the specialists they hire to contain an incident and limit the areas affected. This is an aspect of cyber hygiene that can be continually improved on to help companies respond quickly and minimise damages.

Malicious attacks have increasingly targeted the manufacturing industry, which has been relatively late implementing proper defence mechanisms. The sector also has a lower maturity in operational technology (OT) and industrial control systems (ICS), while their dependency on systems and automation has grown rapidly.

The control systems mentioned above are particularly important as OT systems are integrated with advanced technology, such as sensors and aggregation platforms in modern "smart factories". The fact that these systems have the ability to remotely track and control production in real time increases the exposure in case of a cyber incident.

8/ **Accumulated yearly growth by industry**



	2016	2017	2018	2019	2020	2021
Manufacturing	1	3	9	16	23	43
Financial Institutions	0	7	7	33	14	21
Professional Services	1	4	3	12	19	39
Communication, Media & Technology	3	6	4	9	22	16
Retail / Wholesale	0	2	6	9	12	12

In order to combat the increase in malicious attacks, it's important for manufacturers to invest in cyber resilience as well as purchase cyber insurance. With insurance, the firms will not only gain first- and third-party protection against losses, but also access a suite of tools and services, depending on policy specifics. These tools can include vulnerability scans, penetration tests, and consulting services to help develop a cyber incident response plan.

Cyberattacks can affect manufacturers in various ways, including:

Operational inefficiencies, as disrupting one component can bring all operations to a halt.

Loss of reputation and market share.

Bodily injury and property damage, as hijacking industrial control systems can lead to a dangerous manufacturing environment.

Impaired business growth, through a loss of intellectual property.

INDUSTRY FOCUS: OIL AND GAS

The oil and gas industry depends heavily on technology to gain efficiencies by automating processes and systems. For example, globally, the industry relies on more than 1,000 third parties to support digital transformation. While the industry is nowhere near the top in the number of cyber claims filed, the impact from cyberattacks in this sector could have potentially severe consequences.

Consider that, across all industries, supply chain attacks targeting open source software increased by 650% in 2021 compared to 2020. Experts have suggested three changes to help reduce the operational costs in the oil and gas supply chain: increasing supply chain visibility, improving compliance, and enhancing supplier collaboration.

Cyberattacks on oil and gas control systems can result in unauthorised amendments to software and therefore the processes they control, with significant consequences. The most common cyberattacks facing oil and gas companies are via malware, ransomware, and phishing.

In the US, an attack in 2021 on fuel pipeline operator Colonial Pipeline forced the company to close its network, carrying nearly half of the US East Coast fuel supply, for six days. A prolonged shutdown of the line could have had a serious impact on gasoline prices. Another major attack in Europe, including in Germany, Belgium, and the Netherlands affected dozens of oil and gas facilities around the world.

These types of attacks could potentially extend to national electricity grids and affect safeguards and warning systems with potentially catastrophic losses, including capital asset damage and long-lasting business interruption.

3

Cyber hygiene can help minimise cyber incidents

Insurers closely monitor the cyber threat landscape and evolution of claims, adapt underwriting guidelines, and review organisations' risk management practices. Changes in risk trends and increased exploitation of certain attack surfaces, such as third-party service providers or software, can quickly factor into underwriter discussions regarding an organisation's insurability.

In recent years, the cyber insurance market has experienced increased pricing, reduced capacity, and higher retentions as underwriters focused on companies' cybersecurity posture, which if deemed insufficient could cause insurers to decline coverage. The frequency and severity of ransomware claims has been a significant driver of the challenging conditions — though not the only one — and has led insurers to encourage key cybersecurity controls.

One area in which many companies have a blind spot involves understanding the scope of the relationship between cyber risk and third-party suppliers/vendors. Yet it is a critical area, especially as many organisations work closely with suppliers, integrating them into corporate and/or operational structures in efforts to increase efficiency. Insurers closely monitor the cyber threat landscape and evolution of claims, adapt underwriting guidelines, and review organisations' risk management practices. Changes in risk trends and increased exploitation of certain attack surfaces, such as third-party service providers or software, can quickly factor into underwriter discussions regarding an organisation's insurability.

However, such relationships can increase an organisation's cyber risk and widen the potential attack surface. As organisations plan to integrate vendors into their information technology (IT) networks, they should analyse the supplier's IT infrastructure and its staff training for vulnerabilities.

A recent survey from Marsh and Microsoft found that while organisations take many cybersecurity actions, they widely overlook their vendors/digital supply chains. For example, only 43% of survey respondents had conducted a risk assessment of their vendor/supply chain.

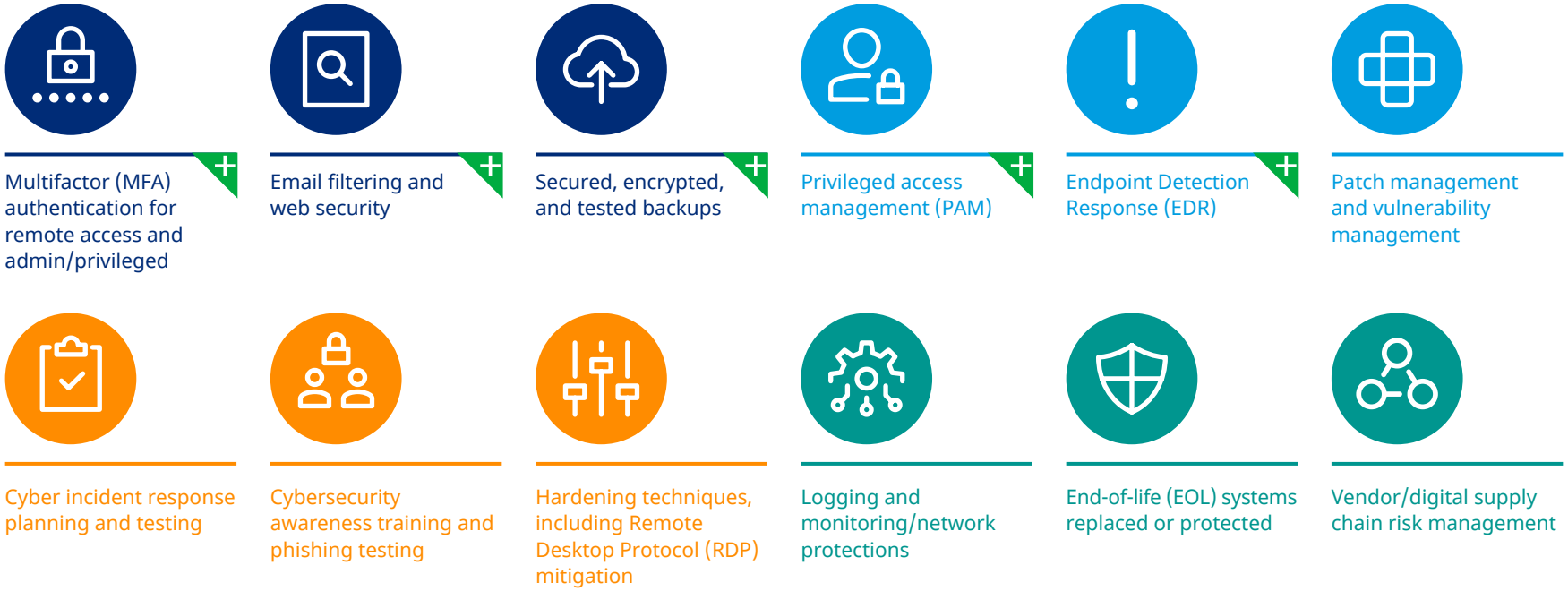
As cyberattacks increase in frequency and severity, underwriters have identified a correlation between certain key controls and cyber incidents. Through such analysis and the continuous examination of relevant data points, the insurance industry is developing a deeper understanding of the technical steps that organisations can take to build cyber resiliency.

However, due to the growth in attritional losses, insurers continue to take a cautious position. Many insurers are tightening their underwriting terms, carefully analysing all cyber insurance applications, and asking more questions than ever before about an applicant's cyber operating environment and risk controls.

Insurers now typically require organisations to adopt specific controls; a failure to adopt them can put insurability at risk. Forward-looking companies now emphasise these controls to help mitigate ransomware and other threats as they improve their overall cybersecurity posture.

Marsh recommends the implementation of 12 key cyber controls, including vendor/digital supply chain risk management, to help address both organisational cybersecurity and insurer concerns in the current market.

Of the 12 controls, insurers have focused on five they indicate as having the greatest positive impact on reducing cyber risk and thus are often required to be insurable:



Supply chain attacks on the rise

The growth in supply chain attacks since 2020 across Europe should concern all organisations. About half of all attacks are carried out by advanced persistence threat (APT) actors, according to the European Union Agency for Cybersecurity (ENISA). The complexity and resources of threat actors require organisations to improve their protective methods and cooperate closely with anyone allowed access to their network and systems.

APTs often focus on a supplier's code to gain access to their customers. ENISA says that over 60% of such attacks took advantage of companies' trust in suppliers. While organisations should work with suppliers they trust, they should still verify the security standards that are in place throughout their supply chain and network.

Any incident within a cyber supply chain can cause cyber business interruption, which can be just as disruptive and costly as a traditional business interruption. An attack on cyber supply chain can put at risk any information, material, or product that flows from the first supplier to the ultimate end user, through any company in the middle of the chain, until the product is sold.

Supply chain attacks typically occur in two phases. During the initial attack, the threat actors gain access to the supplier. Following this, sometimes months later, they will gain access to the customer and the assets they had targeted all along.

The timing of a cyber incident can have a major impact on the amount of lost revenue, and thus on a claim. While a property loss disruption may last for a period of weeks, months, or even years, a cyber incident may only last for a number of hours or days. Such a short period requires accurate and detailed data in order to assess and prove the impact on the operational loss. Loss adjusters usually focus on hourly revenue information, or daily sales, rather than on traditional profit and loss information.

Accumulation of losses is usually a key issue in cyber business interruption claims. While a property damage claim is typically viewed as being at a single physical location, a cyber incident can spread across a network and cause disruption at multiple locations.

Many organisations use the same software or similar components, meaning a cyberattack can affect many entities at once. Many insurers are now addressing cyber risk accumulation exposures through exclusions and restrictions on coverage.

Organisations should update their cybersecurity and incident response plans with supply chain attacks in mind, incorporating all their suppliers — IT and non IT — in their protection and security verification. Insurers have begun to request more detailed information about a company's cyber supply chain, ranging from the names of key IT vendors to questions around compliance of cloud vendors with applicable laws related to data storage and transfer or security measures in place, such as ISO 270001. Recognising this, Marsh's Cyber Self Assessment tool includes a section for vendor management.

What if ...

a cyber incident occurs with a software provider, website builder, or data storage company?

Can you continue operating?

Conclusion

With cyber claims increasing every year, organisations cannot afford to hope that they won't be affected. Companies need to take meaningful steps to ensure their cyber safety, looking beyond their company and into their network.

There has been some positive cybersecurity news of late, such as the global decrease in ransoms being paid and the fall in average losses in the manufacturing sector. And the standards set by financial institutions and healthcare organisations are examples to other industries on how to combat and minimise cyber risks.

Guides such as the 12 key controls continue to contribute to improving cyber hygiene and decreasing accidental incidents, while increasing the ability of firms to manage incidents.

Cyber insurance is now offered by insurers across the globe, and continues to adapt to new market conditions and geopolitical realities. Still, increased cyber vigilance is needed regarding supplier and vendor relationships. Greater cooperation between firms, governments, and software/hardware developers can help to minimise incidents and limit the damage when incidents do occur, something that is easily proposed, but hard to implement.

About Marsh

Marsh is the world's leading insurance broker and risk advisor. With around 45,000 colleagues operating in 130 countries, Marsh serves commercial and individual clients with data-driven risk solutions and advisory services. Marsh is a business of Marsh McLennan (NYSE: MMC), the world's leading professional services firm in the areas of risk, strategy and people. With annual revenue nearly $20 billion, Marsh McLennan helps clients navigate an increasingly dynamic and complex environment through four market-leading businesses: Marsh, Guy Carpenter, Mercer and Oliver Wyman. For more information, visit marsh.com, follow us on LinkedIn and Twitter or subscribe to BRINK.