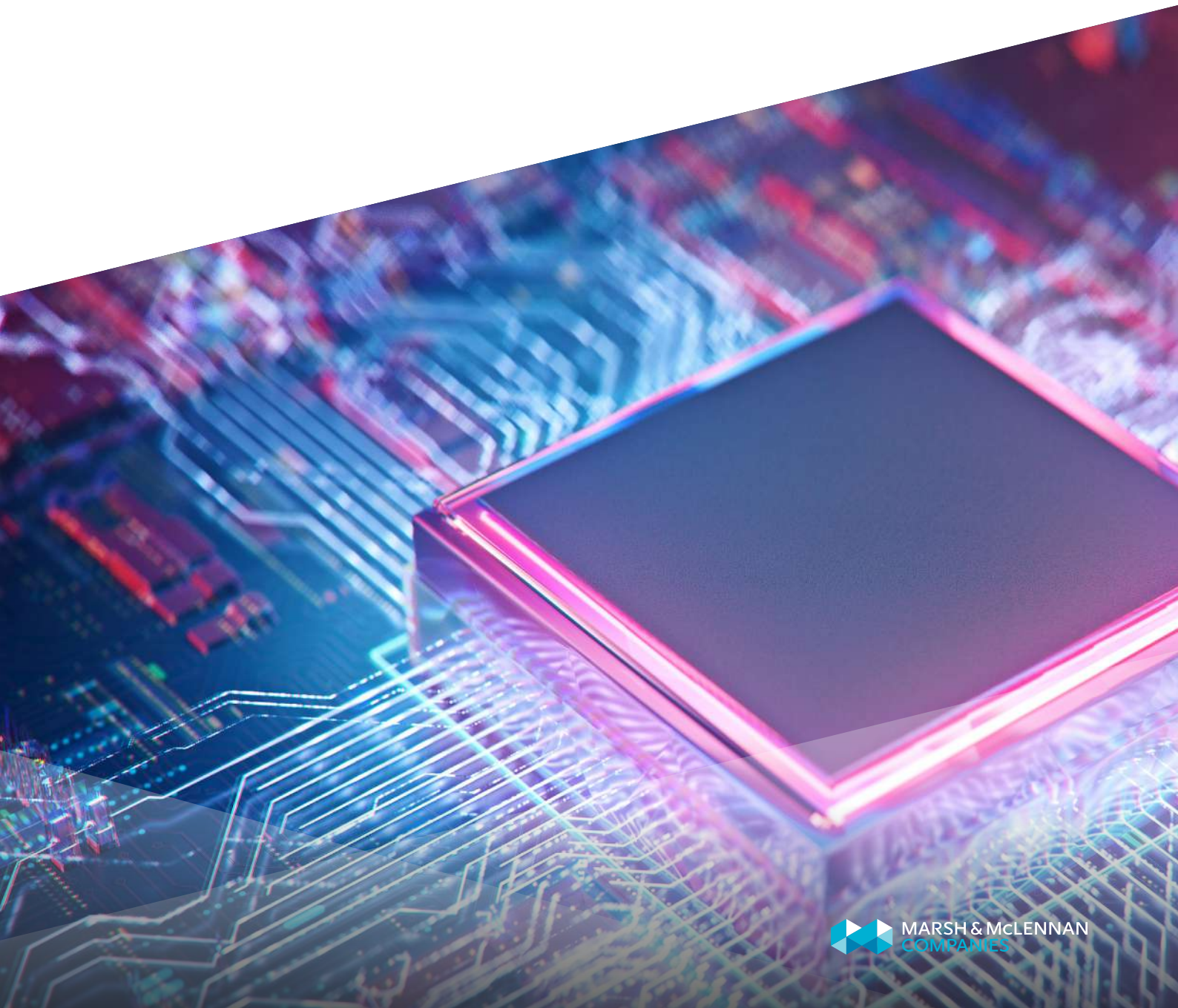
MARSH | WAVESTONE | CMS Law.Tax

CLAIMS SOLUTIONS | JULY 2020

The Changing Face of Cyber Claims

A Cyber insurance loss study in Continental Europe



MARSH & McLENNAN COMPANIES

CLAIMS SOLUTIONS | JULY 2020

The Changing Face of Cyber Claims

A CYBER INSURANCE LOSS STUDY IN CONTINENTAL EUROPE

CONTENTS

Introduction

Digitalisation is revolutionising how companies operate, and driving business leaders to think differently. The pace of technological change keeps increasing, and dramatically transforming the global business environment, with continual advances in areas ranging from artificial intelligence and the Internet of Things (IoT) to data availability and blockchain.

At the same time, the potential cyber and technology exposures that businesses face continue to expand, presenting the possibility for substantial economic losses.

Indeed, in *The Global Risks Report*, produced annually by the World Economic Forum in collaboration with Marsh & McLennan companies cyber risk consistently ranks among the top five concerns for companies around the world. In turn, more companies are purchasing cyber insurance to take advantage of the expanding protections it offers, particularly in light of the indirect consequences of the Covid-19 pandemic — including a boom in remote working.

Organisations increasingly see cyber insurance as a reliable and cost-effective way to transfer the financial risks they face from the expanded use of data and technology in business operations. These include losses and expenses associated with a growing range of cyber perils, such as malicious attacks, privacy breaches, and accidental events.

Cyber policies and cybersecurity should be seen as complementary: While the insurance indemnifies the financial impact, cybersecurity manages the frequency of attack by, for example, keeping malware out of an organisation's IT system.

Over the years, there have also been developments in assistance and prevention services relating to cyber incident management, including IT forensic support, cyber-extortion negotiation experts, and data monitoring support.

In Continental Europe, the cyber insurance market is maturing and the rate of cyber insurance purchasing is increasing rapidly. As we see more claims triggered under these policies, the opportunity to learn about the landscape increases — not only in claims management, but also in incident management — and prevention.

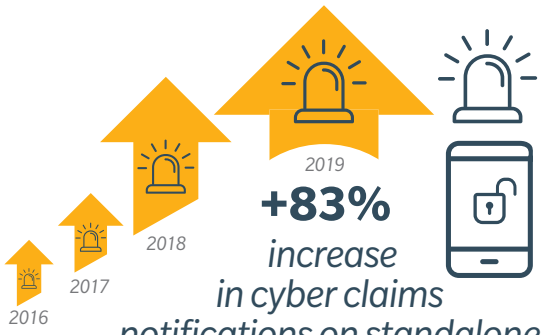
Using the insights gathered from Marsh's claims data and from the data, experience, and expertise from Wavestone and CMS, this report looks at practical ways to manage and mitigate cyber risk and claims.

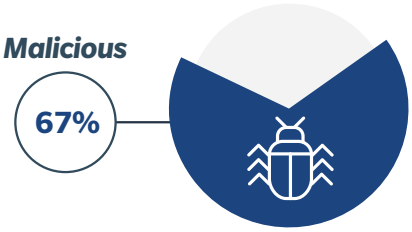
CLAIM TRENDS

Key takeaways from our analysis of hundreds of cyber claims handled by Marsh in Continental Europe.

Cyber claims notifications and insurance indemnification grow exponentially

In Continental Europe, Marsh saw notifications double each year from 2016 to 2018, and grow by 83% in 2019. Despite an increase in purchase rates of standalone cyber insurance, cyber insurance claims, and claim payouts, are increasing at a faster pace than the growth of the number of cyber policies that are being purchased.

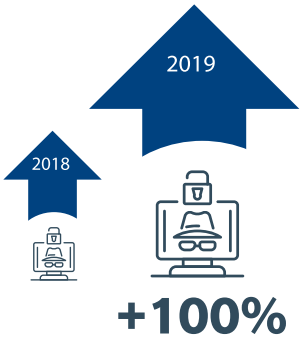




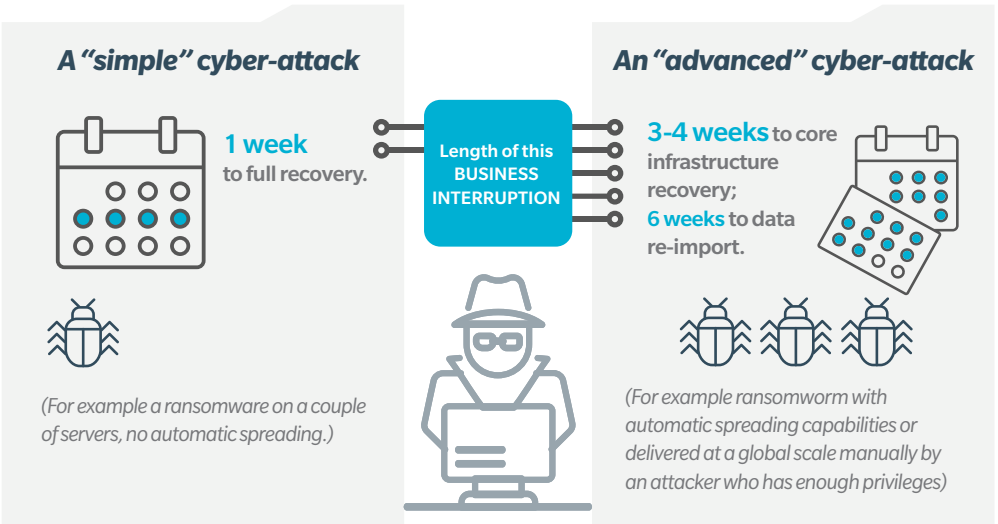
Based on all cyber claims that Marsh analysed, 67% of attacks were malicious and just 28% accidental.

Ransomware on the rise

Our analysis shows that modus operandi of cyber-attackers is changing: ransomware attacks now make up 14% of the total, and when an attacker has successfully delivered their ransomware to a victim, business interruption is always a significant part of the loss.

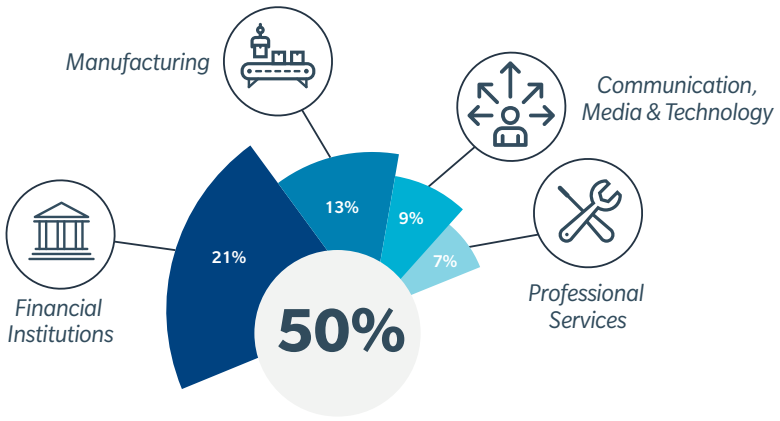


Ransomware
The number of ransomware claims notifications doubled during 2019.



Most affected industries

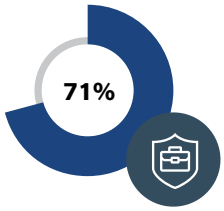
Financial institutions and other companies within financial services are impacted the most by cyber incidents.



Source: Marsh.

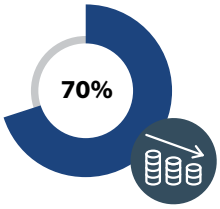
Financial impact

The costs and expenses associated with a cyber incident can be categorised into four segments.



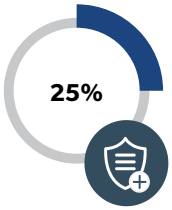
Assistance & Emergency Measures

- Identification, assessment, and containment of security event (IT forensics).
- Provision of legal assistance (data breach of confidentiality).
- Provision of crisis management or communication assistance.



Additional Costs

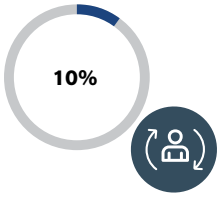
- Restoring the IT system to its state prior to the claim.
- Maintaining operability of the IT system.
- Preparing the claim.
- Preventing or mitigating a liability exposure/detecting and controlling any improper use of personal data (data breach).
- Communication strategy.
- Notification to the authority or to individuals (data breach).
- Ransom.
- Defense costs resulting from an investigation by a regulator.
- Regulatory fines by national authorities for data protection rights violations, such as the GDPR.



Liability Coverage

Defense costs and damages arising out of claims made by third parties:

- A security event.
- A breach of confidentiality of personal data.
- Defamation, damage to reputation, breach of intellectual property, violation of privacy, etc.



Loss of Turnover & Increase in Cost of Work

- Business interruption.
- Extra expenses.

NOTE: Graph shows the frequency of each.

Source: Marsh.

A look ahead

As companies rely more heavily on their IT systems, the business interruption associated with any disruption becomes even more substantial and detrimental. At the same time, ransomware attacks are increasing in sophistication and are even infiltrating backup systems. Cyber insurance can help mitigate the severity of an incident and also the associated costs.

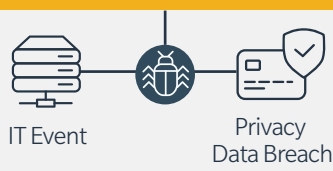
POST-CYBER INCIDENT: KEY PHASES

The timeline following a cyber incident can be broadly split into two phases:

- **The first phase is incident management.** This requires both internal and external expertise in various areas, including IT, legal, and public relations (PR). This is where we metaphorically fight the fire.
- **The second phase is claims management.** On the road to "business as usual", firms will need to lean on another group of experts to facilitate adequate reimbursement of cost from the insurance policy. These include loss adjusters, loss assessors, and claims advocates.

The above is the case whether the incident is associated with an IT event or a privacy data breach. Looking at specific scenarios, we will review the key learnings for incident management and outline a plan of action for claims management.

Cyber Incident Phases



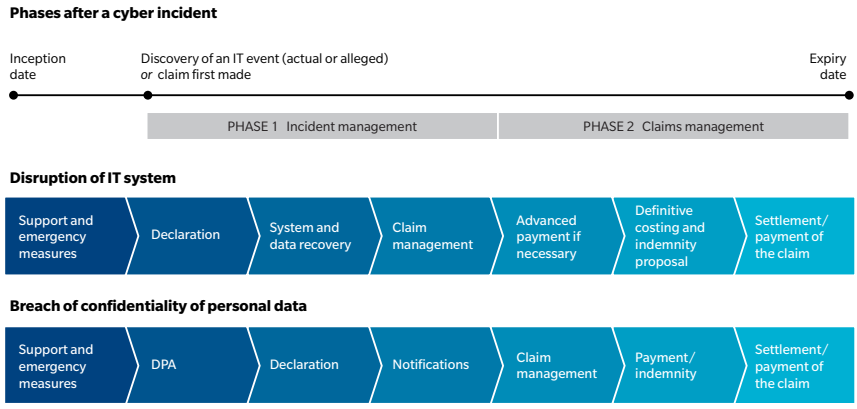
First phase

Incident Management
Internal and external expertise required: IT, legal, and PR.

Second phase

Claims Management
Facilitate adequate reimbursement of costs from the insurance policy: loss adjusters, loss assessors, and claims advocates.

Incident and claims management steps



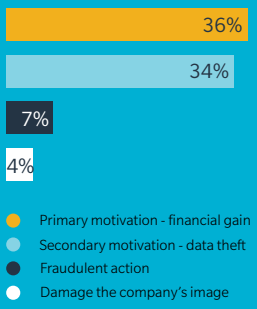
MODUS OPERANDI OF CYBER CRIMINALS

Knowing your enemies is the key to dealing effectively with their attacks. To do so, the CERT-Wavestone has analysed 40 major security incidents that led to the disruption of business activities or an advanced compromise of the information system. The affected entities are organisations among the largest companies and institutions (in the public and private sectors, including retail, information technology, and finance). The following key figures unveil the different modus operandi of cyber criminals and their main motivations.

MOTIVATIONS

Financial gain remains the driving force for cyber criminals

Research carried out by Wavestone shows that the **primary motivation** for cyber-attackers remains **financial gain.** Data shows that the largest proportion of incidents were **ransomware (36%)**, followed some distance behind by the financial gain motivation of **fraudulent action (7%)**. The second motivation for attackers is **data theft** — both business and technical **(34%)**. A small percentage of the attacks analysed **(4%)** aimed to **damage** the **company's image** through the defacement of websites and theft of social network accounts, and 4% of the compromises aim to gain new attack capabilities: bypassing security mechanisms, attacks on trusted partners, and illegal eavesdropping of the network example.



DURATION OF INFILTRATION

164 days is the average time elapsed between an intrusion and its actual detection.

According to the Wavestone research, many organisations still struggle to detect intrusions. Indeed, **35% of companies** failed to **detect** intrusion incidents.

When cross-referenced with detection methods, the findings are even more worrying: **Only 26% of security incidents are identified** by the company's cybersecurity detection service.

In **44% of cases**, it is the **employees** who are **alerting directly** — but often too late.

Incident Management

Ransomware infection combined with IT disruption

Scenario

- A major firm in the industrial sector is infected with ransomware.
- IT services, such as internet, emails, and business applications are unavailable for a week.

Financial consequences

- Crisis management costs.
- Business continuity impact.

DISRUPTION OF IT

The first step in managing an incident involving an IT system disruption is to enable support and emergency measures. This can be done by calling the insurer-provided crisis hotline that is listed in the policy. Depending on the extent of the incident, IT forensics experts will be deployed, who will analyse the incident, its origins, and its consequences in order to limit or contain the impact. Crisis management or communication consultants might also play a role, depending on the insured's needs. Generally, the faster the crisis hotline is called the better the incident can be contained.

After an attack, IT systems cannot be used in a normal manner, so usage must be fully or partly stopped to allow for cleaning or rebuilding. In some cases, attackers destroy critical parts of the IT infrastructure; in other cases they penetrate and propagate the IT system for weeks to steal data or corrupt internal systems. This is known as an "advanced persistent threat" and it causes a loss of confidence in the IT system.

To add to this, many organisations do not have significant distance between everyday IT systems and backup/recovery IT systems.

As a result, in the event of a major cyber-attack, the recovery systems are often compromised alongside the everyday IT systems. This happens for three main reasons:

1. Replication systems could copy the malware between the main IT estate and the recovery systems.
2. Attackers could exploit the administration infrastructure, common across the two systems, to propagate within both.
3. Even where recovery systems are fully isolated, attackers could still exploit vulnerabilities present within both; then, triggering recovery systems would open the door for the malware to spread.

To tackle loss of confidence in IT systems — both everyday and recovery — business continuity and disaster recovery planning is needed.

To date, such plans have responded to scenarios like physical datacentre destruction; many do not cater for major cyber-attack scenarios and the resulting loss of confidence in an organisation's IT systems. Now, business continuity plans and disaster recovery plans need to be reworked to face cyber threats.

For an organisation to be cyber-resilient, when faced with a major cyber-attack it must be able to maintain vital activities in a downgraded mode — all while taking actions to quickly regain confidence in the IT system so as to return to normal operation.

Wavestone outlines that there are three areas of preparation that businesses should focus on ahead of an incident to achieve this resilience.

PREPARE TO CONTAIN THE ATTACK WHEN IT OCCURS

It is necessary to carry out the organisational and technical actions below to contain the attack when it occurs.

Organisational actions:

- Identify the necessary people to call upon during a crisis (for example, management, forensic experts, IT department, legal department, HR, and communications team) and specify their roles and responsibilities.
- Define processes that allow quick decisions from operational teams for threat containment (such as systems shutdown and floodgate activation) that do not require crisis management team (CMT) sign-off.
- Define appropriate processes that enable investigation and defence-plan-related activities, and ensure around the clock operations.

Technical actions:

- Identify backup communication tools outside of normal IT to safely manage the crisis, as the usual communication tools may be compromised.
- Make sure you have adequate means to analyse and understand the attack, such as sufficient, safe and searchable logs; capability to analyse unknown malware; and technical and functional cartography.
- Define floodgates in your network to be able to limit the attack propagation by isolating the most sensitive systems from those already compromised.
- Make sure you have the right tools to protect the parts of the IT estate that are still safe once the threat has been isolated, for example, quick patch deployment.

It is also essential to regularly test the cyber-crisis management process via crisis exercises using ambitious and realistic scenarios.

PREPARE TO WORK WITHOUT IT

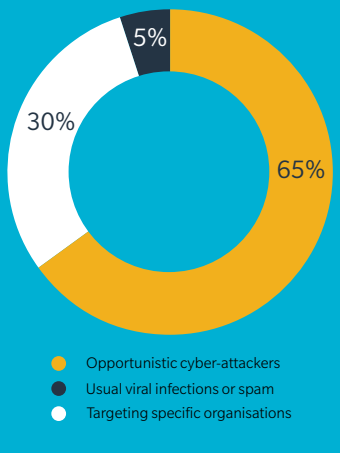
Business teams need to learn how to work in a downgraded mode to simulate IT systems being unavailable or untrustworthy for a few days or weeks.

THE TARGETS

More than 50% of attackers do not have advanced technical skills.

Despite the rise of spear ransomware attacks worldwide and in Continental Europe, the research shows that **most cyber-attackers are opportunistic (65%).** They do not demonstrate highly technical skills or do not target a specific organisation. They seek out and abuse systems that are poorly protected and easily attacked. These attacks could be avoided if security measures were more robust. **Of the 30% of managed attacks targeting specific organisations**, the aim is to obtain sensitive and accurate information from within the organisation.

The final **5% of the attacks** correspond with the **usual viral infections or spam.** They do not target a specific organisation and have a limited effect on the information system, such as denial of service or loss of user data.



VULNERABILITIES

The same entry points are regularly used by attackers to penetrate their targets' information systems

The human element remains a significant vulnerability when it comes to cyber-attacks. Although large companies have better ways to protect their employees, they may not always be able to effectively protect their customers, partners, or SMEs in their ecosystem.

Therefore, phishing is still one of the main vectors of cybercrime thanks to its very low attack cost and quick results. According to Microsoft, phishing attacks increased by 250% in 2019.*

Phishing aims to steal sensitive data and even large companies with advanced protection can fall victim to "spear-phishing", where the phishing email is tailor-made to attract the employees of a particular department. In a third of cases, the attacker exploits a vulnerable web application. In fact, a Wavestone study outlines that **100% of web applications are vulnerable**, and act as easily accessible gateways.

*SOURCE: https://info.microsoft.com/ww-landing-M365-SIR-v24-Report-eBook.html?lcid=en-us

At such, business teams should ask themselves the following key questions to define processes and tools accordingly:

- Can we operate with manual workarounds? If not, how can we interrupt our business activities in a controlled manner?
- What data do we need?
- What alternative tools do we need?

These alternative ways of working must be tested to ensure the continuity of essential activities in the event of a major cyber-attack.

PREPARE TO REBUILD YOUR IT

If important parts of the IT estate cannot be cleaned of a malware infection, there may be a need to rebuild some workstations, applications, or infrastructure to maintain vital business activities. This must be anticipated, and processes and tools must be defined and implemented accordingly.

For workstations, in situations where remote restore is not available, user-friendly packages (USB key and documentation) can be created to allow end-users to rebuild their workstations themselves. Mobile backup servers can also be used to restore a user's data. For applications and infrastructure, the key to success relies on two points:

- Rebuilding must be prioritised according to pre-defined business needs.
- Architectures must be standardised as much as possible to help automate and simplify their deployment if they need to be rebuilt.

Do not forget standard cybersecurity measures, without which cyber-resilience cannot be fully complete.

Implementing these preparatory measures will help improve cyber-resilience, but efforts must go hand-in-hand with obtaining appropriate protection and the monitoring of IT systems.

Incident Management Takeaways

Disruption of IT

The first step in an incident involving IT system disruption is to enable support and emergency measures.
After an attack, IT systems cannot be used normally.
An "advanced persistent threat" causes a loss of confidence in the IT system.

Prepare to contain the attack when it occurs

Organisational actions:
- Identify the necessary people to call.
- Define processes that allow quick decisions.
- Define appropriate processes.

Technical actions:
- Dentify backup communication tools.
- Make sure you have adequate investigation.
- Define floodgates in your network.

Prepare to work without IT

Can we operate with manual workarounds?
If not, how can we interrupt our business activities in a controlled manner?
What data do we need? What alternative tools do we need?

Prepare to rebuild IT

Rebuilding must be prioritised according to pre-defined business needs.
Architectures must be standardised as much as possible to help automate and simplify their deployment if they need to be rebuilt.

FOCUS ON PRIVACY DATA BREACHES

Managing personal data breaches in practice

International law firm CMS is appointed by numerous organisations across all sectors and several major cyber insurance carriers as the first response legal advisor in relation to data breaches. Below are some practical insights, based on CMS's experience of advising on hundreds of cybersecurity incidents.

The EU General Data Protection Regulation (GDPR) is wide in its application. Many cyber incidents qualify as personal data breaches under its definitions. The GDPR requires organisations to implement measures to have appropriate technical and organisational measures in place to address data breaches, and to keep records of all breaches that have occurred under their responsibility. When it is likely that a breach could result in risks to individuals (which could include fraud or reputational damages), the supervisory authority must be notified without delay and where feasible within 72 hours of becoming aware of the breach. Where the level of such risk to the rights and freedoms of natural persons is likely to be "high", the data subject (the natural person to whom the data relates) must additionally be notified without undue delay.

ASSESSING THE INCIDENT

A first step in every cyber incident is to assess if it may result or has resulted in a breach of security leading to the accidental or unlawful loss of confidentiality, availability, or integrity of personal data. If it has, the second step is to assess whether the data breach may result in a risk to the rights and freedoms of natural persons. This should be done by looking at the nature of the breach and the type and amount of data involved. A forensic investigation is often required to assess what has happened and the potential risks arising from a breach. Consequently, close collaboration in multi-disciplinary teams is needed; typically this includes the insured's management and IT staff, assisted by an external team of IT and legal experts. Involvement of the organisation's data protection officer is also recommended.

DEALING WITH A LACK OF INFORMATION – BETTER SAFE THAN SORRY?

A common challenge when conducting forensic investigations is the ability to quickly determine the source of the incident and its consequences, for example, a lack of relevant logging data, either because it is stored for a limited time after the incident or is not stored at all. In the case of a ransomware attack, for example, it may be necessary to pinpoint the malware's properties and network logging data to assess whether the incident has potentially resulted in a transfer of personal data outside the network. Sometimes, due to a lack of logging data, it may be unclear whether a discovered software vulnerability has resulted in a security incident at all. Difficulties in assessing the nature and severity of an incident can put an organisation in a difficult position when deciding whether or not to notify supervisory authorities and/or data subjects, especially under the pressure of strict notification deadlines. While organisations grapple with potential consequences of non-compliance on the one hand and a risk of unnecessary notifications on the other, CMS observes that some authorities are taking the general position that the presence of risk must be assumed unless there is proof that no such risk exists. This approach does not follow directly from the express text of the GDPR, so future case law will need to clarify whether this approach is correct. This strategy however seems to result in organisations making a substantial number of "better safe than sorry" notifications and waiting to see if the supervisory authority will follow up or not. In the Netherlands for example, based on case studies, CMS estimates that approximately 60% of all reported breaches fall within this category.

SOURCE: CMS Enforcement Tracker, European Union, May 2020, www.enforcementtracker.com

NOTIFY ON TIME

As statutory and contractual obligations typically give tight deadlines for notifying a personal data breach, a key question is when an organisation must be considered to have become aware of the breach. As notification deadlines will in practice be no longer than 72 hours, many organisations still struggle to promptly recognize cyber incidents as personal data breaches. There is a legal risk of non-compliance with GDPR or contractual obligations if a breach appears to be notifiable and is not notified in time. It is therefore important to involve first response advisors urgently upon discovering incidents to reduce such risk.

Even when a notifiable breach is recognised in a timely manner, communicating all required information within the applicable timeframe can remain challenging, especially where deep forensic investigation is required. In terms of GDPR compliance, this is not necessarily a problem because the GDPR allows for preliminary notifications. The experience is that authorities tend to deal with this flexibly – as long as the follow-up notification is provided promptly.

Where a breach is likely to result in a high risk to data subjects, they also need to be notified of the incident without undue delay. Such notification is often made after notifying the supervisory authority, but sometimes they are informed even within a couple of hours, for example in case of compromised credit card data or official identification documents. As these kinds of incidents tend to result in potential fraud soon after the data is compromised, it is crucial that data subjects are notified in order to take precautionary measures.

IDENTIFY CROSS-BORDER ISSUES

Cross-border data breaches involving multiple EEA jurisdictions are particularly difficult to navigate, as they can trigger the need to involve multiple authorities. In such circumstances, the GDPR provides a "one-stop-shop" principle: an organisation need only make one single notification to the supervisory authority in the jurisdiction where it has its so-called "main establishment" (as defined in the GDPR) in the context of the relevant processing. However, benefiting from this principle is only possible where such main establishment is clearly identified. This identification process has frequently been overlooked in an organisation's GDPR implementation project and ad-hoc identification may sometimes be impossible within the given timeframes. Some organisations are unexpectedly faced with the time consuming and expensive need to notify authorities in multiple jurisdictions and in different (local) languages. We highly recommend identifying main establishments and lead authorities for data processing operations well before a breach.

PR STRATEGY

Data subjects are becoming more aware of their rights under the GDPR and are increasingly responding to breach notifications with damage claims and data access requests. A well-considered PR strategy and external communications support can help streamline communications and mitigate against these consequential legal risks (and costs), especially when dealing with large numbers of data subjects.

BE READY FOR FOLLOW-UP

Organisations should always remember that information provided in breach notifications can be used later to substantiate a supervisory authority's investigations and enforcement decisions. They can come back into the picture even months after notification of the breach. Sometimes they request additional information or instruct the data-controlling organisation to inform data subjects if it has not yet happened. The authority will possibly start investigations into whether the breach notification and the level of security of the organisation are GDPR compliant, and this can be followed by sanctions. According to the CMS Enforcement Tracker, which tracks publicly announced fines made under the GDPR, roughly 25% of all sanctions are related to a lack of adequate security measures.

A diligent and strategic approach before notifying supervisory authorities is therefore advisable. In a recent case, the notification of a data breach by a large Belgian telecommunications operator resulted in the supervisory authority launching an investigation into the position and independence of the operator's Data Protection Officer. In turn, the supervisory authority concluded that the Data Protection Officer was not sufficiently independent, and imposed a EUR 50.000 fine. In this regard, a final point to be aware of is that the notification of a breach may be a trigger for the supervisory authority to investigate an organisation's compliance with other GDPR obligations which are not even related to the notified breach.

Top 3

EU countries by number of fines

1st Spain
2nd Romania
3rd Germany

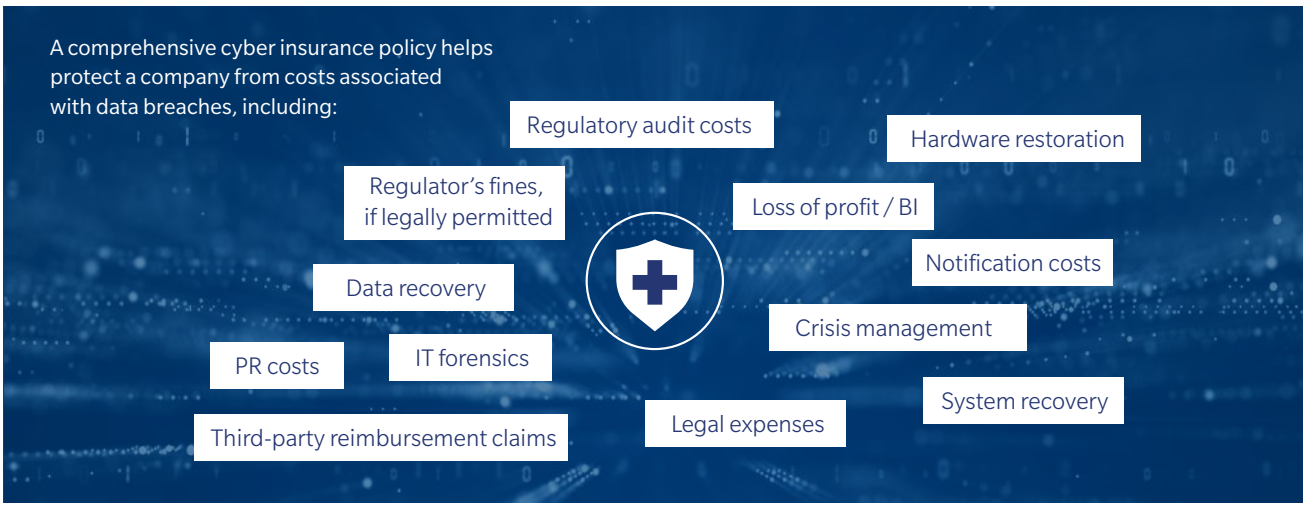
Top 3

largest individual fines

1st France
2nd Italy
3rd Austria

Approximately **25%** *of fines relate to* ***insufficient data security*** *and around* ***4%*** *to* ***non-compliance*** *with breach notification obligations*

SOURCE: CMS Enforcement Tracker, European Union, May 2020, www.enforcementtracker.com



A cyber insurance loss study in Continental Europe

Claims Management

Web application compromise leading to a data breach

Scenario

- Law enforcement seizes a server belonging to attackers and discovers data from a retail company.
- Law enforcement raises an alert to the company, which then carries out an investigation to identify the extent of the compromise.
- All of the company's customer databases were stolen, including credit card data. This data was subsequently used to perform frauds on other services.
- The breach was due to an inadequately secured web application.

Financial consequences

- Investigations costs.
- Communication with clients.
- Fines due to non-compliance with PCI DSS/credit card data protection security rules.

THE PROCESS

After the IT forensic experts have begun to analyse the incident and assist with vital mitigation activities, the organisation declares the claim to the insurer and loss adjusters are appointed. As system and data recovery progresses, the claims management process starts.

Fees and loss amounts are consolidated, the valuation and assessment of the claim is prepared, and the coverage is reviewed. This can take several weeks. If necessary, advance payments are made, before the definitive costing and indemnity proposal is presented.

Garnered from several years of cyber claims experience, here are several key areas — applicable to both business interruption and data breach claims — that can be addressed well before a cyber loss occurs.

PRE-LOSS ACTIVITIES

To be better equipped for this area of risk, there are various pre-loss activities that can be carried out involving the broker, the carrier, and the insured.

- Make sure that you have the right cyber insurance cover, with sufficient limits, that is fit for your business and complementary to the other policies you have.
- If you would like to call on vendors and service providers that are not part of the insurer-provided vendor network, ensure that this is separately endorsed in the policy.
- It is also very important for both placement and claims teams to have an onboarding meeting with you as soon as a policy is bound; this is to explain the insurance coverage and to share best practice.

Organisations may not be at ease with cyber claims, as they may not have experienced these types of losses before.

There are two key ways your team can make this a smoother process, if a cyber incident were to occur.

- A formalised cyber claims protocol can be very beneficial to organisations during a cyber-related crisis. This will set out the internal procedure with your key actors, including your chief information security officer, insurance department, legal department, and finance.
- A named loss assessor/forensic accountant because cyber claims are very often multisubsidiary and spread out geographically.

POST-CYBER INCIDENT ACTIVITIES

Once the crisis phase is over, and the cyber policy coverage has been triggered, the insurance claims management process kicks off. Your broker should be informed of the claim in parallel to the call to the crisis hotline — they will be needed for a successful claim settlement. We encourage the involvement of your broker in the claims management process; cyber insurance can be complex as it combines a variety of first-party and third-party risk coverage.

Originally, cyber insurance predominantly focused on data privacy liability breaches; as such, a large portion of cyber claims are handled within the financial lines claims department, which has limited first-party claims experience. First-party related cyber claims, however, represent the vast majority of the claims in Continental Europe. The involvement of PD/BI claims departments is often necessary in Europe.

There are a number of useful actors in the claims management process.

- Cross-disciplinary team: Where a cyber incident is felt in various geographies, coverage may be triggered across the breadth of the policy, in multiple jurisdictions. These claims are generally best handled by international cross-disciplinary claims teams, consisting of experts from liability, financial lines, and first-party lines.
- Single point of contact: Ideally, in these instances you will have a single point of contact coordinating activities across various actors and experts. The key tasks of the advocates are to ensure that the insurance policy responds as intended, and the indemnity payable is optimised and paid in the shortest possible timeframe.
- Forensic accountant: These are financial experts, who will prepare and quantify the claim for the client. This can entail estimating the compensation period, and calculating and analysing the business interruption components with the aim to present the claim to insurers in an agreeable way.

Below we list further advice from our claims experts that can help deliver a smoother claims handling experience:

- Compensation period: Create a timeline of all events from when the security incident took place to the total recovery of activities, in order to precisely determine the compensation period. This is because some events are discovered months after the actual infraction, and to be able to illustrate the costs and impact of the incident, all the events need to be linked. In some instances, insureds have incurred costs for sometime an the incident, and it has been challenging to negotiate with insurers that these costs were linked to the event.
- Collection of proof: It is important that you have all invoices and supportive documents to present to loss adjusters. The invoices need to be detailed, especially when external consultants have been used, so that you can justify that their involvement was for the cyber incident management only.
- Quantification of BI: Quantifying business interruption is different to quantifying the costs of external consultants as there is no supporting invoice. The impact on sales, gross margin, and additional costs incurred to reduce the business interruption will all need to be calculated. Historical data and financial reporting is very important for a meaningful evaluation here.
- Third-party claims: Claims from a third party may also be part of the claim quantum. It is recommended that you quantify the potential damages payable due to contractual breaches. In other cases, where the affected party is not the responsible party, one can quantify the potential damages that can be claimed from the responsible party.

CONCLUSION

Cyber insurance is a fast growing market. As digitalisation and interconnectivity increases within our society, and between our organisations, so will the risks that come with them. We expect the purchase rates of cyber insurance will increase over the coming years. As a result of higher cyber insurance uptake, the number of claims we at Marsh handle will also rise.

Moving forward, Marsh, alongside both Wavestone and CMS, will continue to learn from our clients' needs and questions, and from the claims we handle, in order to assist organisations in becoming more cyber-resilient.

ABOUT MARSH

Marsh is the world's leading insurance broker and risk adviser. With over 35,000 colleagues operating in more than 130 countries, Marsh serves commercial and individual clients with data driven risk solutions and advisory services. Marsh is a wholly owned subsidiary of Marsh & McLennan Companies (NYSE: MMC), the leading global professional services firm in the areas of risk, strategy and people. With annual revenue over US$15 billion and 75,000 colleagues worldwide, MMC helps clients navigate an increasingly dynamic and complex environment through four market-leading firms: Marsh, Guy Carpenter, Mercer, and Oliver Wyman. Follow Marsh on Twitter @MarshGlobal; LinkedIn; Facebook; and YouTube, or subscribe to *BRINK*.

ABOUT WAVESTONE

In a world where knowing how to drive transformation is the key to success, Wavestone's mission is to inform and guide large companies and organisations in their most critical transformations, with the ambition of a positive outcome for all stakeholders. That's what we call "The Positive Way." Wavestone draws on over 3,000 employees across 8 countries. It is a leading independent player in European consulting.

In response to new challenges induced by cybercrimes on the rise, Wavestone supports its customers in securing their digital transformation from the strategic phases to the operational implementation, while offering an appropriate response in the event of an attack. In order to best meet the needs of a wide range of clients, the 500 Wavestone cybersecurity consultants combine functional, sectoral and technical expertise, covering more than 1,000 engagements per year in 20 countries.

A proven expertise in: Risk Management & strategy, Digital compliance, Cloud & Next-Gen security, Ethical hacking, Incident response and Digital Identity for users & customers, especially in the field of financial services, manufacturing & industry 4.0, IoT & consumer goods.

ABOUT CMS

Founded in 1999, CMS is an integrated, multi-jurisdictional organisation of law firms that offers full-service legal and tax advice. With more than 70 offices in over 40 countries across the world and more than 4,800 lawyers, CMS has long-standing expertise both in advising in its local jurisdictions and across borders. From major multinationals and mid-caps to enterprising start-ups, CMS provides the technical rigour, strategic excellence and long-term partnership to keep each client ahead in its chosen markets.

The CMS member firms provide a wide range of expertise across 19 practice areas and sectors, including Corporate/ M&A, Energy & Climate Change, Funds, Life Sciences & Healthcare, Technology Media and Communications, Tax, Banking & Finance, Commercial, Competition & EU, Dispute Resolution, Employment & Pensions, Intellectual Property and Real Estate & Construction. Visit cms.law

For further information, please contact your local Marsh office or visit our website at marsh.com.

JEAN BAYON DE LA TOUR
Head of Cyber – Continental Europe
MARSH
T: +49 152 0162 6445 | M: +33 7 78 51 15 74
jean.bayondelatour@marsh.com

TARA HILLFRAM
Head of Claims Advocacy – Continental Europe
MARSH
T: +49 (0)711 2380 584 | M: +49 (0)1520 1627 584
tara.hillfram@marsh.com

VINCENT NGUYEN
Head of Cert-w
WAVESTONE
T: +33 (0)1 49 03 20 00 | M: +33 7 62 83 13 61
vincent.nguyen@wavestone.com

GRACE ANG-LYGATE
Senior Business Development Manager,
Technology, Media & Communications
CMS
T: +44 20 7367 3921
grace.ang-lygate@cms-cmno.com