Cyber claims analysis report

Turning data into insight

Cyber claims analysis report

Turning data into insight

Table of contents

Introduction and executive summary

At Willis Towers Watson we continuously analyse claims reported by our clients. This enables us to understand the nature, trends, causes and cost breakdown of loss events impacting businesses. This report uses our analysed claims data to provide specific insight into the types of loss that your business may be exposed to. All claims that we have analysed are included in the calculation for the average claim settlement, the determination of the largest loss and the loss amount distribution charts. However, due to the distorting impact of very large losses, we remove "outliers" from the other charts within the report.

Claims reported by clients from 2013 to December 2019 are included in this report:

- This is a total of close to 1,200 claims from nearly 50 countries.
- The average settled cyber claim (where any type of cost has been incurred, excluding zero value losses) is $4.88m.

From this we have seen that:

- Data breaches are the most frequently reported losses and have the largest total amount of costs associated with them.
- Malicious data breaches carried out by third-parties (as opposed to accidental data breaches by the company or malicious data breaches carried out by rogue employees) are the most frequently occurring and most expensive type of data breach loss.

There is a huge variation in the size of data breach losses that we see, ranging from a single data subject to over a million impacted records. Whilst claims in this area are clearly divergent, the following can be discerned:

- The mean number of breached records per claim is over 693,000, whilst the median is much lower at 135.
- Nearly one in ten breaches involved more than 20,000 records.
- From our analysis, the direct event cost per breached record is $7.95.
- For 10% of settled claims, the total cost (including defence costs/other expenses) exceeded $2.5m.

Understanding the scale of the larger claims and the impact they can have on a business is crucial. Whilst losses costing over $10m make up only 5% of claims by volume, they account for 95% of total costs.

Third parties (often suppliers who store data on clients or employees) are responsible for 38% of data breach losses. It is therefore vital to perform the necessary assessments of your third party suppliers' network security and have the correct indemnities in place with these parties. Human error is the next most frequently occurring root cause, leading to 29% of data breach claims. This often relates to employees clicking on links in phishing e-mails or replying to a spoofed e-mail. Employee training is critical here. If you are carrying out "phishing" or social engineering training, consider surveying employees on how that training is performing.

First party risks to insureds are dominated by business disruption and ransomware claims:

- There has been a very noticeable increase in ransomware events in 2019.
- This low investment, low risk and high reward method of cybercrime looks set to continue to grow.
- An example of developments in this area is "ransomware-as-a-service" where ransomware operators share their offerings with other cybercriminals, who then distribute the malware and take a share of ransoms that are eventually paid.
- It is recommended that you have a detailed Disaster Recovery Plan to address ransomware attacks (network disruption) and run table-top exercises testing the plan. Don't let your first true incident be your first test of the plan.

Third party supplier risk is again the dominant cause of claims:

- Third party supplier risk led to 28% of first party losses.
- For nearly one in ten settled first party losses, the total settlement cost (including specialist costs and other expenses) exceeded $2.5m.
- Whilst losses costing over $5m account for only 3% of claims/losses by volume, they account for 63% of total costs.

Social engineering losses (also known as payment diversion, account impersonation/takeover) are also worth highlighting:

- The most frequently notified social engineering event is still that of impersonation of a vendor/supplier.
- The costliest events are typically those that involve impersonation of a CEO/senior manager.
- Although often notified to cyber liability policies, unless the cyber policy contains a specific social engineering/fraudulent transfer insuring clause, coverage may be limited.
- Crime policies can provide wider coverage, but the specific policy language needs to be checked.

In terms of how cyber insurance policies have responded across the various types of claims that have been reported, we have seen that 71% of the average data breach loss falls within the coverage provided by cyber policies, increasing to 75% for first party losses. Two of the most frequently seen coverage issues related to either the use of unapproved vendors or acting without insurers' consent. A good understanding of the policy, early communication with insurers and awareness of the approved vendor lists or gaining insurer pre-approval for your selected vendors will help ensure that these type of coverage issues can be prevented. Utilising modelling and quantification tools will assess your cyber exposure and help you select the most appropriate retention and limits.

Peter Foster
Chairman, Global FINEX Cyber and Cyber Risk Solutions
peter.foster@willistowerswatson.com

Cyber claims overview and headline figures

Figure 1. **Cyber claims analysed global impact**

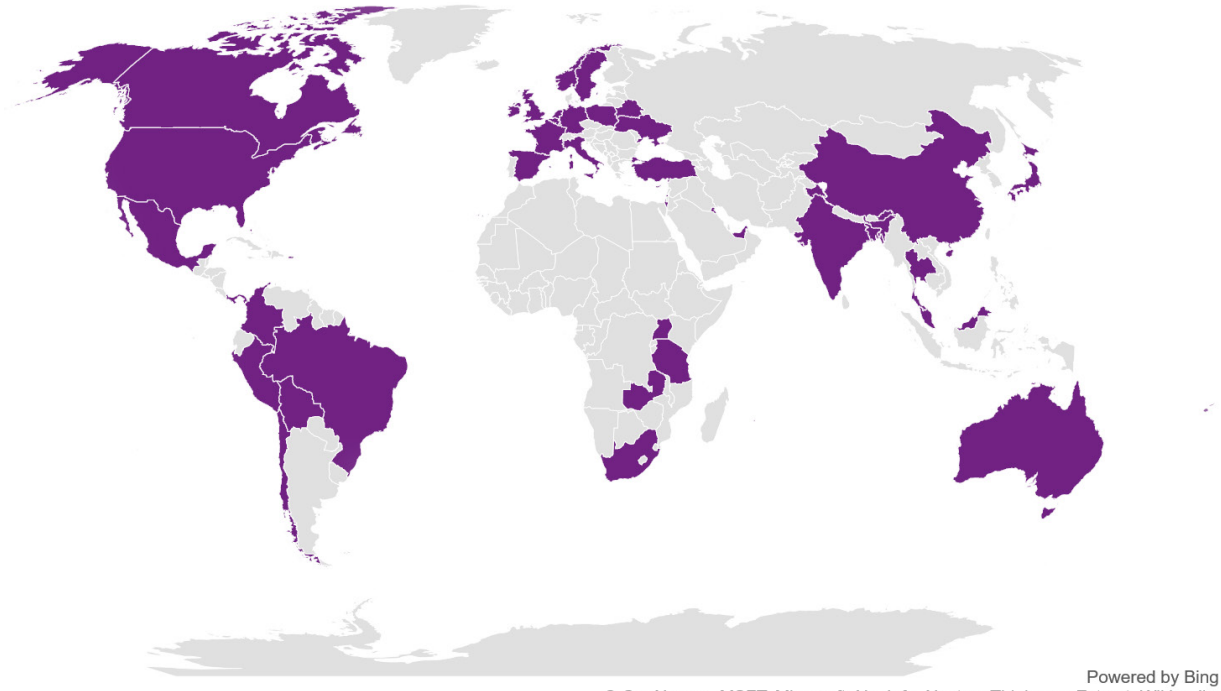
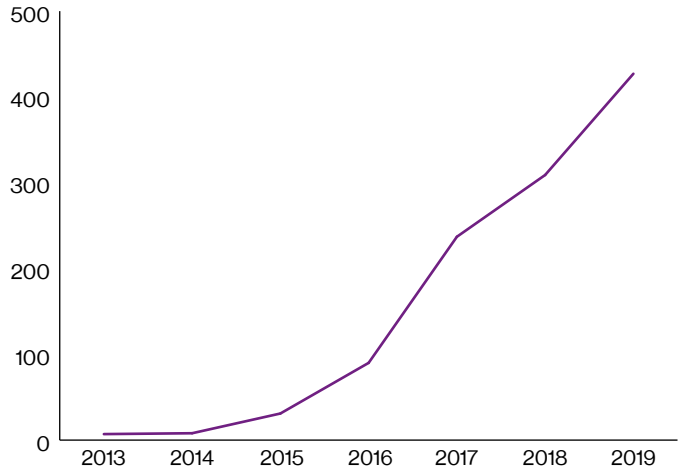


Figure 1 shows the loss locations for the claims analysed.

Figure 2. **Cyber claims notifications by year**



Headline figures

1150+
analysed claims

Average claim settlement
$4.88m

Loss events

Overall, the chart shows that **data breaches** are the most frequently reported losses and have the largest total amount of costs associated with them. A further break down of data breach losses follows on the next page.

Business disruption and **ransomware** events have a high average severity. Although very different in origins, both these types of losses have the ability to severely affect productivity in an organisation and can therefore end up being very costly.

There has been a very noticeable increase in **ransomware** events in 2019. This low investment, low risk and high reward method of cybercrime has the added benefit to the criminals of the anonymity provided by receiving ransom payments in their chosen cryptocurrency. As long as these factors remain unchanged, we can expect to see a continuing increase in these attacks.

Social engineering frauds are no longer just aiming to obtain funds via fraudulent transfer instructions. This method is now also being used to divert salary payments and fraudulently obtain tax data on employees. However, the most frequently notified social engineering event is still that of impersonation of a vendor/supplier. The costliest events are typically those that involve impersonation of a CEO/senior manager.

Figure 3. **Loss events**

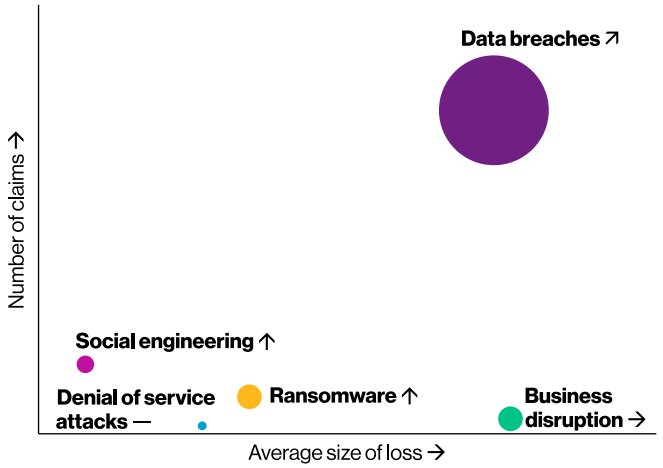
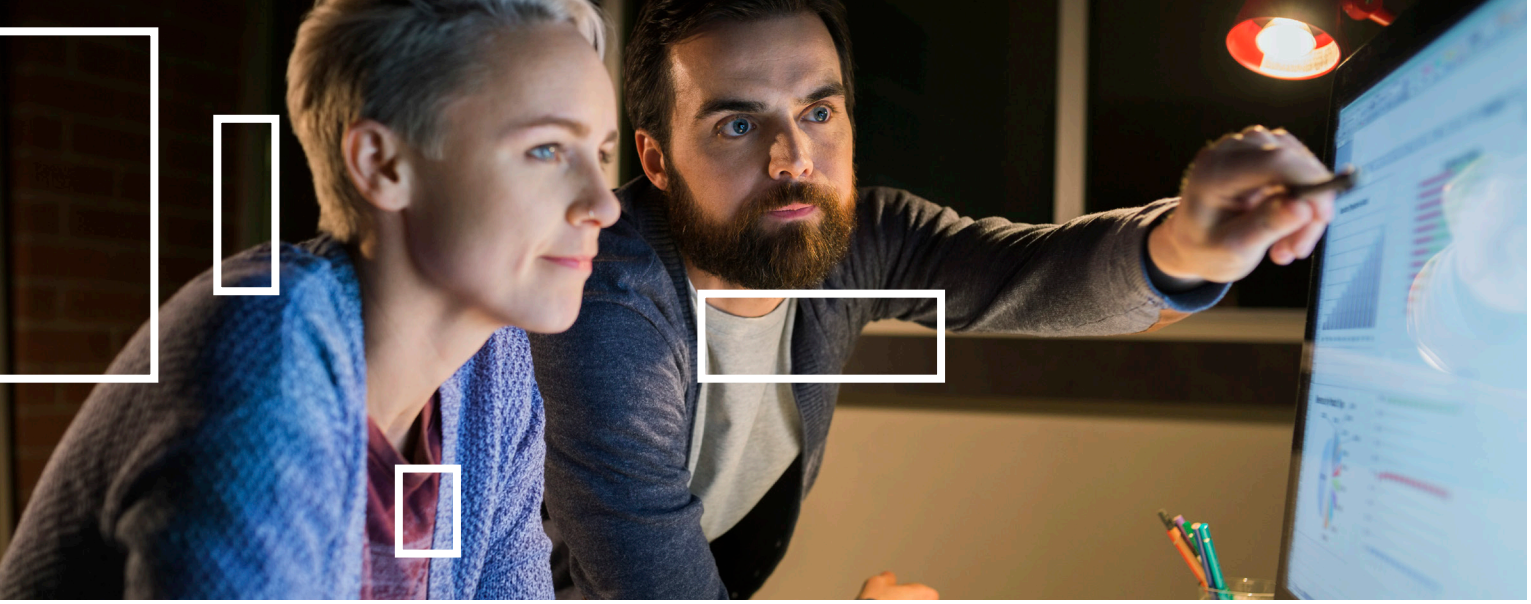


Figure 3 shows the top loss events by both frequency (vertical axis) and average size of loss (horizontal axis). The size of the bubble represents the total cost of each loss event category. The trend arrow shown next to the loss event category shows how the position of the bubble has shifted since the previous year.



Data breaches, in depth analysis

Data breaches come in many different forms, from sending e-mails with client details to unintended recipients, to hackers infiltrating systems to obtain payment card information.

Figure 4 shows how these different types of losses rank in terms of frequency and severity. Perhaps counterintuitively, the analysis has shown that data breaches involving non-financial/medical records are some of the most expensive types of breaches. As shown in the graph below, this is driven by the high number of records breached for these types of events, rather than the sensitive nature of the data. Figure 5 shows the average number of records breached for each different event type.

Figure 4. **Data breaches**

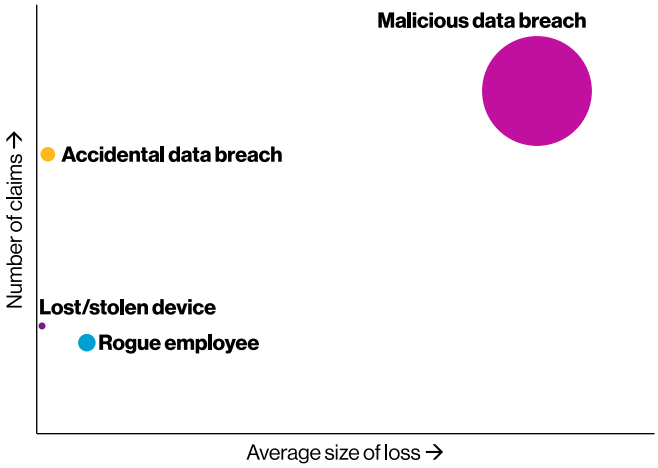
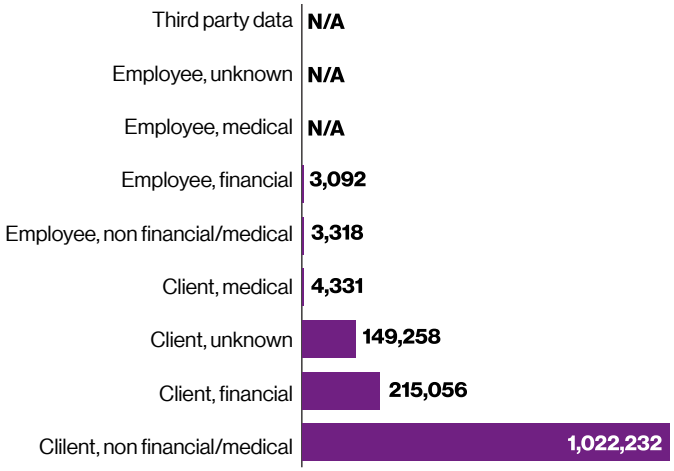


Figure 5. **Data breaches by type**



Data breaches – number of records

Figure 6 shows the distribution of the number of records breached for claims made under cyber policies. It shows that just 8% of breaches involved more than 50,000 records.

From our analysis, the **direct event cost per breached record is $7.95.** Figure 7 shows how the average cost per breached record varies according to the number of records breached. This shows that when there are a lower number of records impacted the costs per record are relatively high. When the breach involves a higher number of records there are economies of scale (due to many crisis management and investigation costs being more fixed in nature) which reduce the costs per record significantly.

Data breaches – root causes

Figure 8 shows the different root causes for data breach claims. It shows that **human error** is the most frequently occurring root cause. This often relates to employees clicking on links in phishing e-mails or replying to a spoofed e-mail. Training and educating employees are key to preventing these types of losses.

Nearly one in four claims where a root cause has been identified have been caused by a **security breach at a third party.** These are often suppliers who store data on clients or employees. The frequency of these events means that it is vital to have the correct indemnities in place with these parties as the responsibility of notifying the customer or employee in the event of a data breach is not necessarily transferred to the supplier when the work is outsourced.

This is in contrast with the **third party** root cause where there was not a case of a security breach at a third party but instead a third party accidentally disclosed data.

Inadequate IT security measures. In these situations, the lack of IT security meant that hackers could access the insured's system directly. Frequently seen scenarios in this category are the failure to install updated security patches or lack of password protocols.

Controls framework root causes are often associated with procedures and protocols regarding verfication of communications. Often these protocols are in place but the pressures of day-to-day work means that they are not followed.

Examples of **non-security related IT** root causes are incorrect disposal of IT equipment, programming errors or poor system design.

Figure 6. **Data breaches by number of records**

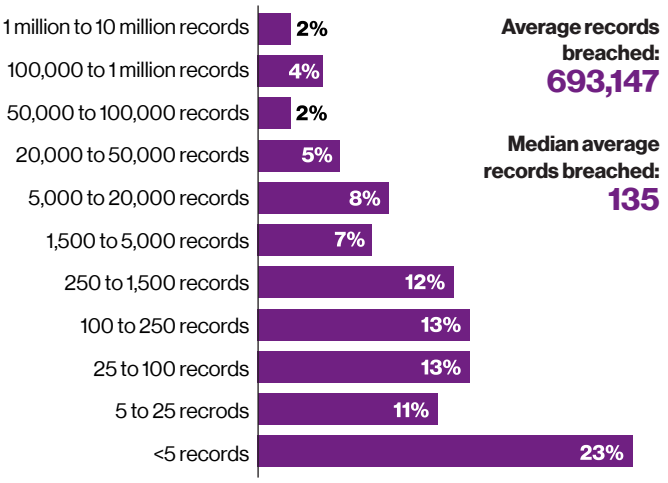


Figure 7. **Average cost per breach**

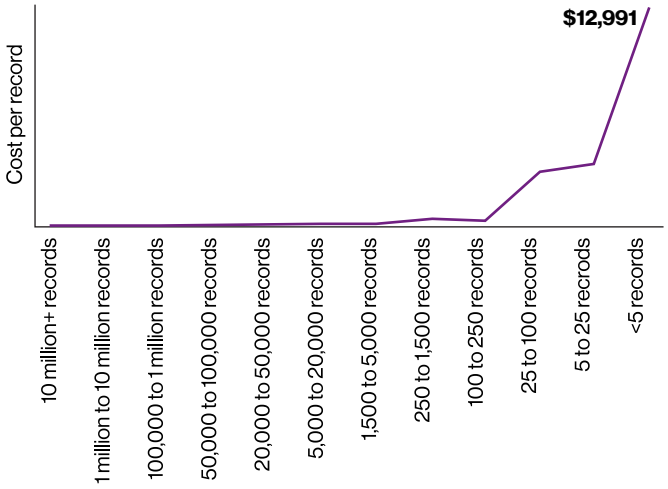


Figure 8. **Root cause of a breach**

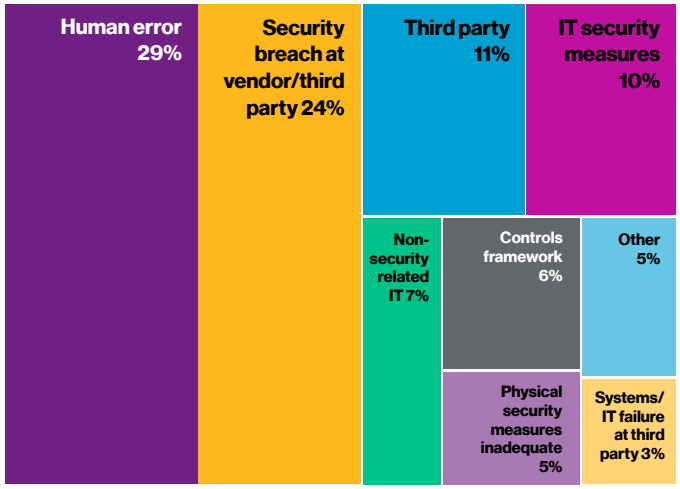
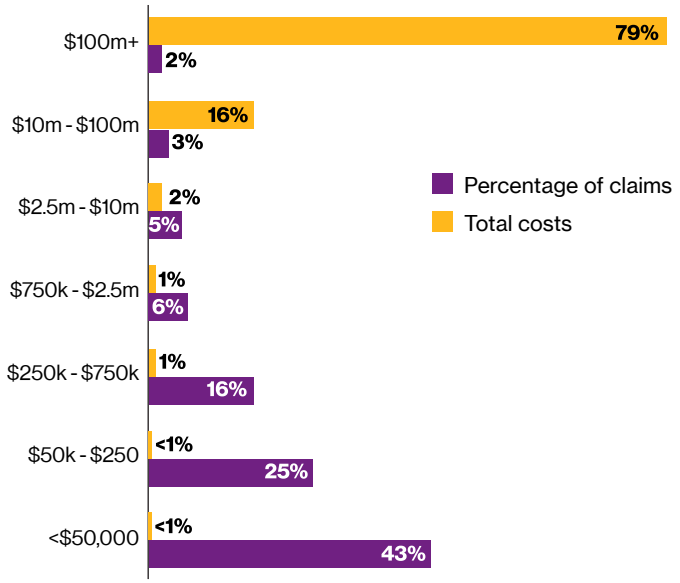


Figure 9. **Distribution of data breach losses**



Data breaches – cost of claims

Figure 9 shows the distribution of data breach losses in terms of their total cost. It shows that for one in 10 settled claims, the total cost (including defence costs and other expenses) exceeded $2.5m.

Figure 10 shows how the average data breach claim is funded. It can be seen that 71% of the average data breach loss falls within the coverage provided by cyber policies; this is made up of insurer payments (44% of the average loss) and insured payments within the retention (27% of the average loss). This highlights the need for an insured to select retention/excess levels which genuinely reflect their willingness/ability to retain risk. Loss modelling/quantification would assist in selecting the most appropriate limits and retentions. See also page 13 for further details of losses not covered.

Figure 11 shows the same average costs but broken down by the different types of cost that they are comprised of.

Figure 10. **Data breach claim funds**

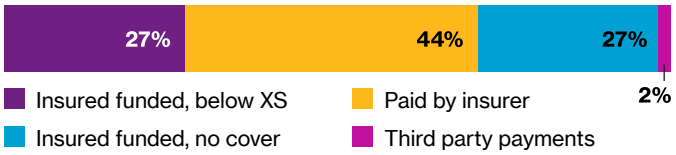


Figure 11. **Data breach claim funds**

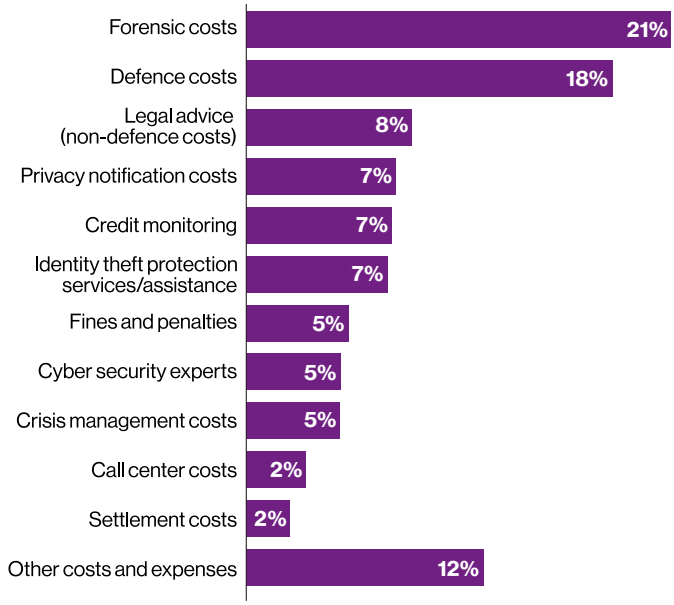


Figure 12. **Typical data breach event**

First party losses, in depth analysis

Figure 13. **First party cyber losses**

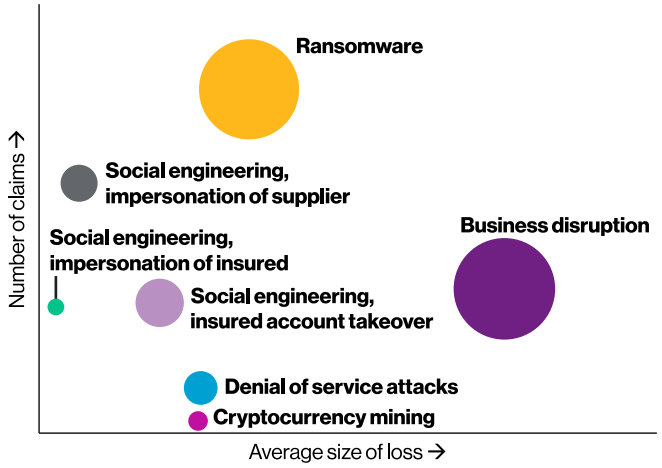


Figure 13 shows the loss events for first party cyber losses by both frequency (vertical axis) and average size of loss (horizontal axis). The size of the bubble represents the total costs of each loss event category. The social engineering loss events have been split out by the different types of losses seen in this category. Account takeover generally refers to e-mail account compromises which are subsequently exploited to cause further losses.

Figure 14 shows the root causes associated with the first party cyber losses. This shows that human error and inadequate IT security measures are the most frequently identified root causes for first party losses. Exposures to third party security breaches or downtime are also significant risks associated with these types of loss. Figure 15 reveals significant financial losses per day with ransomware and other disruptions of business incurring the most extreme costs.

Figure 14. **Root causes**

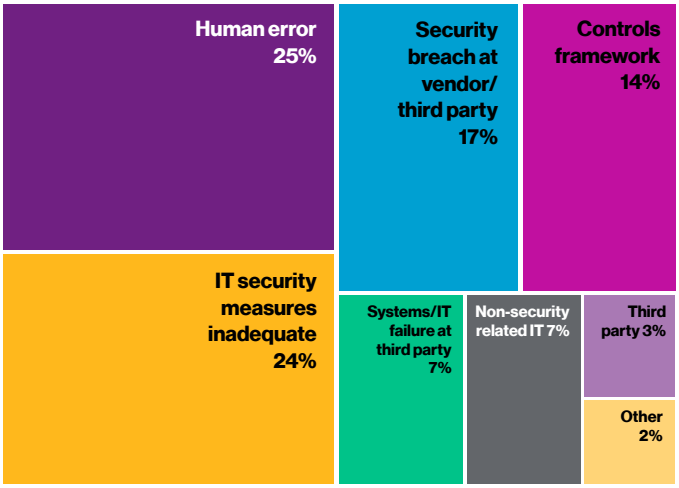


Figure 15. **Costs per day**

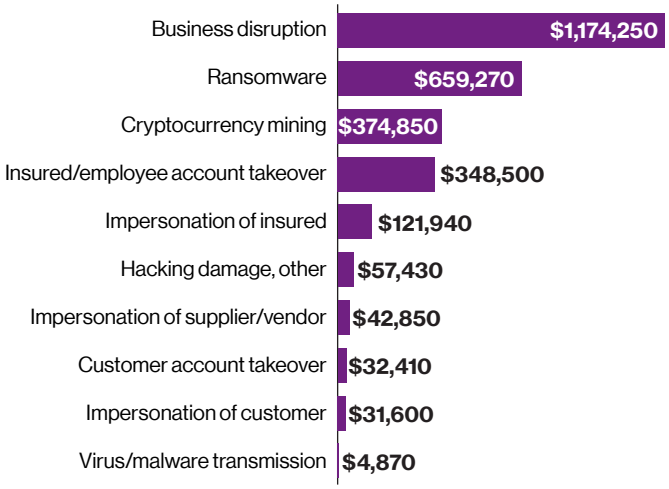


Figure 16. **Cost of claims**

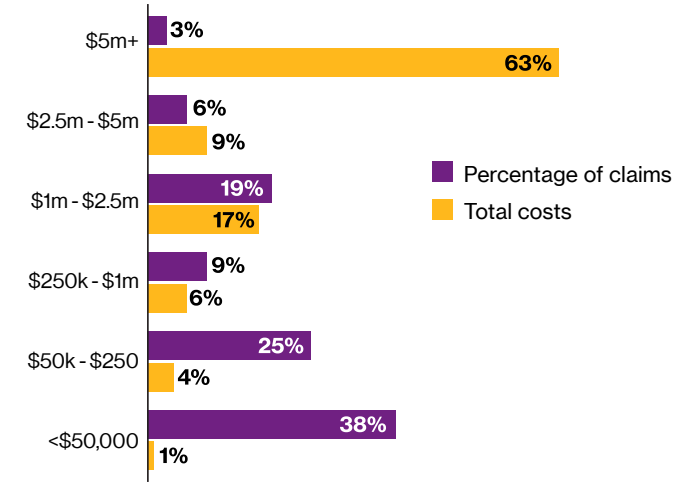


Figure 17. **Cost of claims by type**

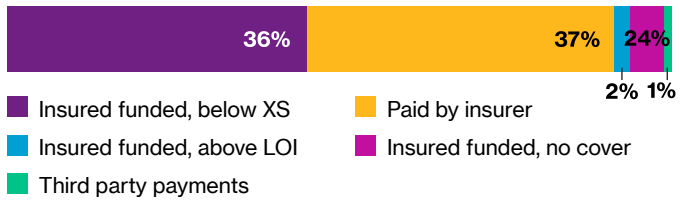


Figure 16 shows the distribution of first party losses in terms of their total cost. It shows that for nearly one in ten settled claims, the total cost (including defence costs and other expenses) exceeded $2.5m.

Figure 17 shows how the average first party claim is funded. It can be seen that 75% of the average first party cyber loss falls within the coverage provided by cyber policies. This is made up of three elements. Insurer payments account for 37% of the average loss. Insured payments within the retention make up 36% of the average loss, highlighting the need for an insured to select retention/excess levels which genuinely reflect their willingness/ability to retain risk. Lastly, 2% of the average loss which would otherwise be covered is not paid by insurers as the loss exceeded the limit of indemnity purchased. It is important that the amount of cover purchased is aligned with the insured's willingness to absorb part (potentially a large part) of a major loss. See also page 13 for further details of losses not covered.

Figure 18 shows the same average costs but broken down by the different types of cost that they are comprised of.

Figure 19 shows the different components that make up the operational/trading costs. It shows that the cost of replacement equipment is generally minimal and the cost of additional resources to rectify outages is the largest cost component.

Figure 18. **Operational costs**

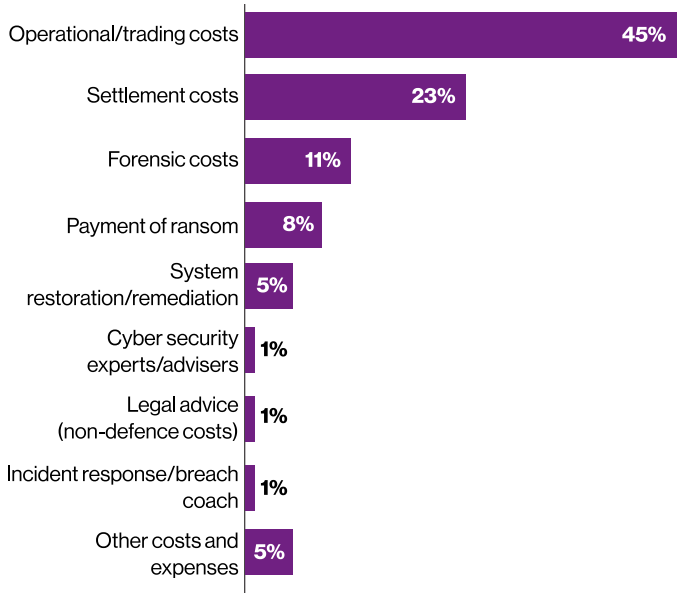


Figure 19. **Operational cost components**

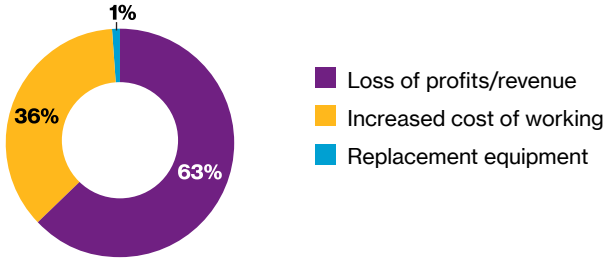


Figure 20. **Typical data breach event**

Claims overview

Figure 21. **Coverage exclusions**

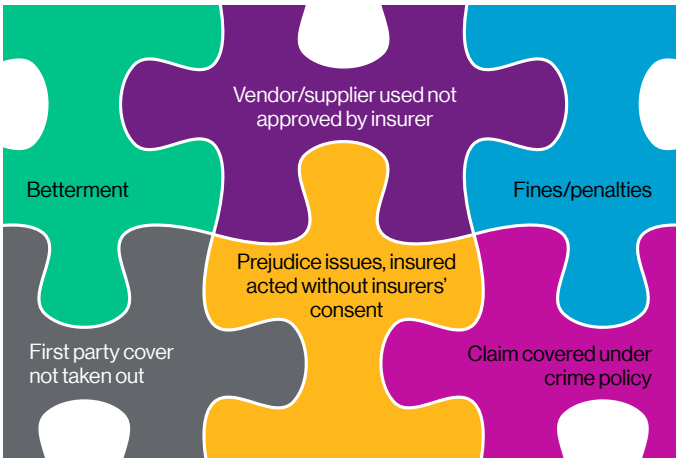
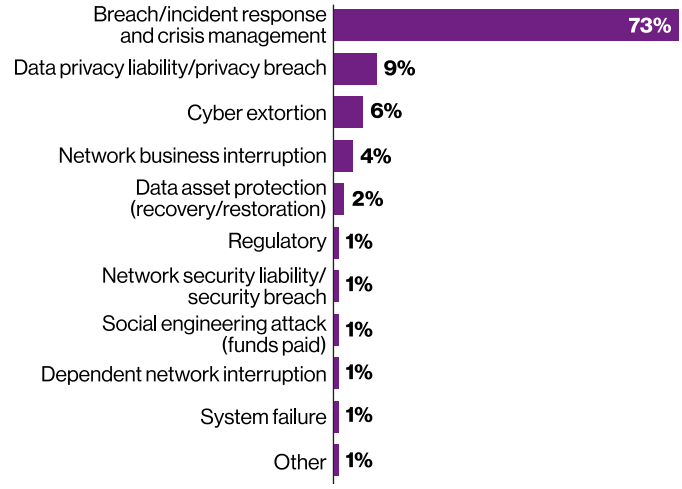


Figure 22. **Insuring clauses**



Coverage exclusions

The average cost funding charts (see pages 8 and 11) show that certain elements of the insurance claims were excluded from cover, in both data breach (27%) and first party losses (24%). Figure 21 shows the most frequently seen exclusions/ reasons why the policy coverage was not triggered.

Two of the most frequently seen coverage issues related to either the use of unapproved vendors or acting without insurers' consent. A good understanding of the policy, early communication with insurers and awareness of the approved vendor lists will help ensure that these type of coverage issues can be prevented.

Policy response

Figure 22 shows the insuring clauses under which cover was confirmed by insurers for all cyber claims. The high percentage of triggered breach/incident response & crisis management clauses highlights insurers' proactive and cooperative approach to having breaches investigated and remediated at an early stage.

Figure 23. **Frequency by industry**

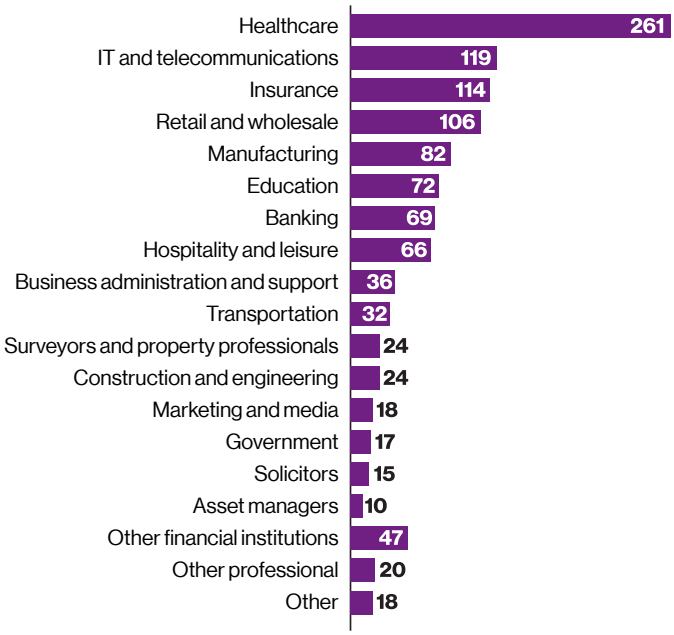


Figure 24. **Loss events**

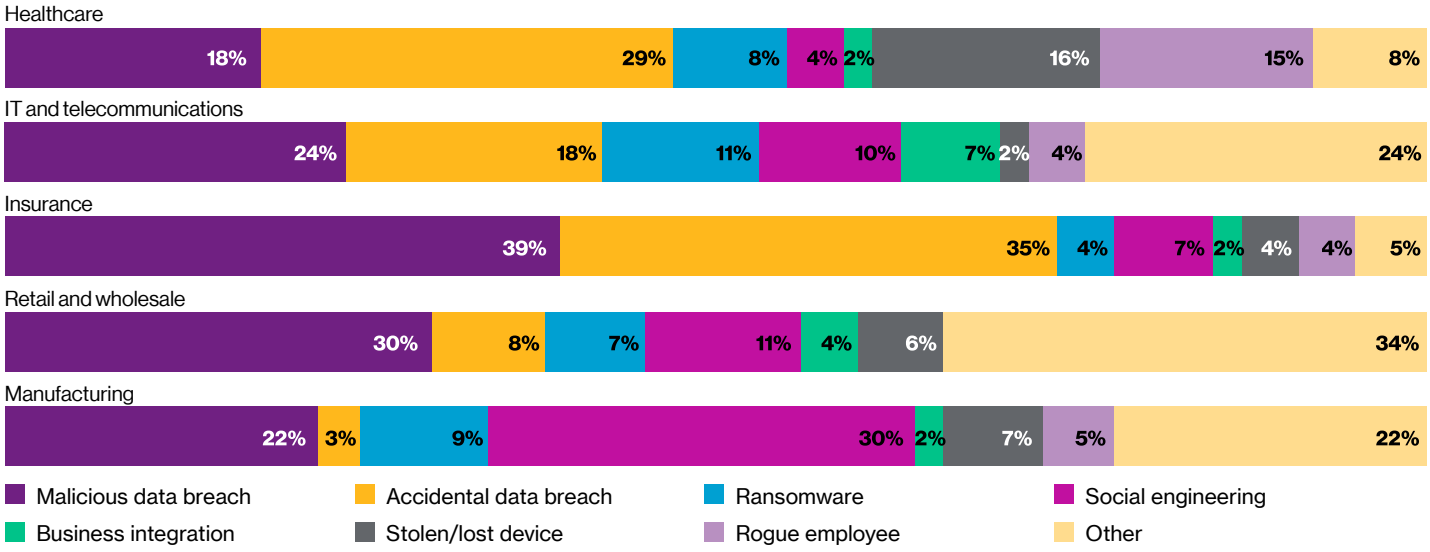


Figure 24 shows the different loss events for the five industries that have reported the most cyber claims. It highlights the different nature of the losses suffered by each of the industry groups.

Claim events profile

Figures 25-28 show the different themes that are prevalent for cyber losses in their respective categories.

Figure 25. **Methods**

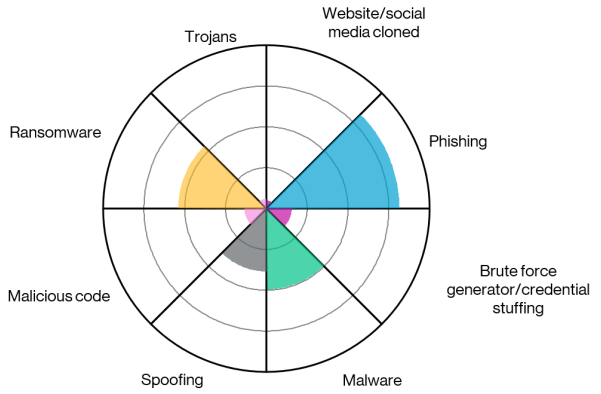


Figure 26. **Type of data targeted/disclosed**

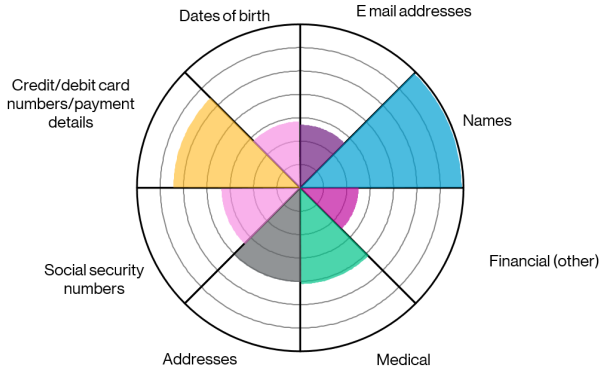


Figure 27. **Background**

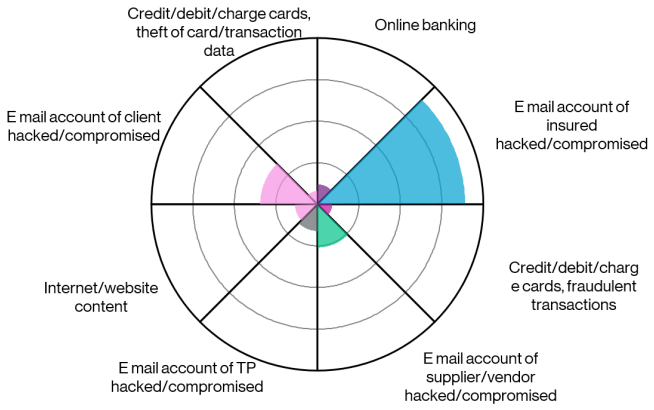
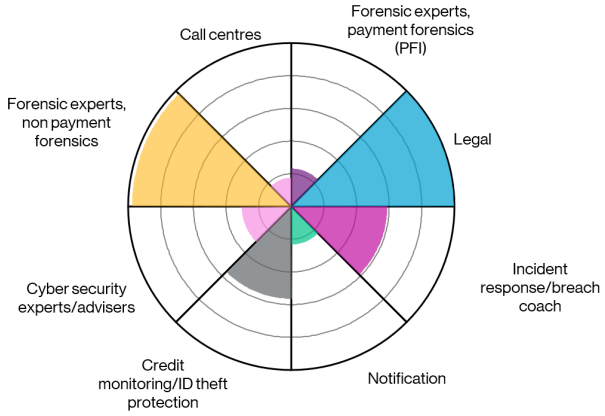


Figure 28. **Appointed vendors**



Claim timelines

Figure 29 shows the average timeline for a cyber claim. It shows that on average the breach/loss lasts about 61 days and it then takes a further 17 days to discover the loss/ breach. Figure 30 shows the average time for the different types of cyber loss event.

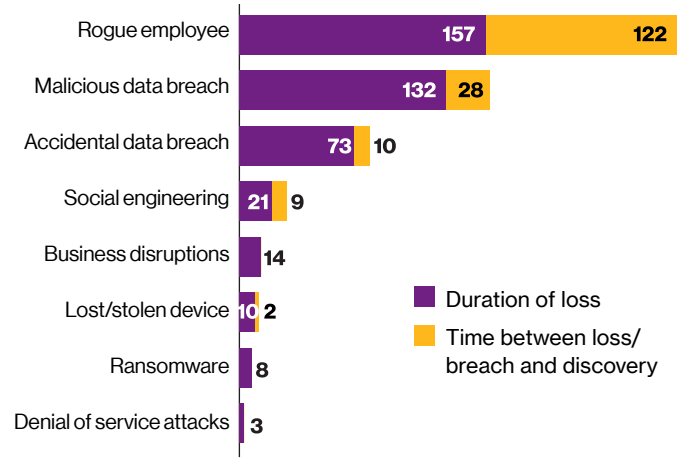
Figure 30 highlights the longer duration and increased discovery time for events caused by rogue employees. This is often due to the fact that the perpetrators are in a position to cover up their actions.

For malicious client data breaches, it shows that on average, the perpetrators will be extracting or accessing data for over four months and that it takes another month to discover that the breach event has taken place.

Loss event types that have a more direct impact on the business, such as ransomware, denial of service attacks and business interruption have shorter timelines both for the duration of the event and the time it takes to discover them.

Figure 29. **Timeline**

Figure 30. **Events caused by rogue employees**



Appendix

Claims examples

Rogue employee – total event cost $14m

The insured discovered that an employee had stolen financial client data. The employee's contract was terminated and the relevant regulatory authorities were advised of the incident. The insured appointed various vendors in relation to the data breach, including forensic, notification, credit monitoring and legal. Multiple regulatory bodies initiated an investigation of the matter. The insured was fined, all affected clients were informed and identity theft protection was offered. All costs were covered by the cyber insurance policy after erosion of the applicable deductible.

Accidental disclosure of data – total event cost $12m

The insured discovered an inadvertent breach of customer non-public personal information (NPPI) as a result of an internal process that provided information to the courts relating to bankruptcy cases. The insured was informed that the redaction on the electronic documents that they filed with the bankruptcy courts was not working adequately. The insured investigated its filing practices and discovered a technical issue with its processes for redacting documents which contained personal information. The insured self-reported the matter to the relevant regulatory body who initiated an investigation into the matter. Vendors were appointed to review all documentation filed by the insured over the years and a large scale re-redaction exercise was necessary.

Ransomware – total event cost $6m

The insured reported that ransomware was discovered within its network on a subset of quality assurance and development servers, virtual machines, desktops and laptops. The insured discovered that data stored where the ransomware resided was encrypted and that it was unable to access the data. The insured subsequently received a ransom demand. The insured carried out risk mitigation activities such as the restoration of servers to back up versions and sanitization and reimaging of the PCs. Public relations, breach coach, and forensic vendors were engaged.

Cryptocurrency mining – total event cost $2m

The insured discovered that it had experienced a bitcoin-mining malware attack in its non-production environments after it investigated an unexplained system slowdown. The insured experienced a similar incident in its production environment and disabled the compromised accounts and ports. To determine the cause and scope of the incident, the insured engaged a third party forensic expert. The forensic experts confirmed that while there was evidence of unauthorized access to certain systems of the insured, they did not find any evidence of access to or acquisition of data. The insured incurred forensic costs, loss of profits and legal costs.

Malicious data breach – total event cost $300m

The insured was subject to a sophisticated hack which led to a data compromise of several million of its current and former customers. The attackers gained unauthorized access of the insured's IT system and had obtained personal information of current and former customers of the insured. The issue was discovered when one of the employees of the insured noticed a database query being run using his credentials. The employee stopped the query and notified the insured's information security department. Vendors were appointed to provide forensic, IT security, credit monitoring, call centre and public relations services.

This report offers a general overview of its subject matter. It does not necessarily address every aspect of its subject or every product available in the market. It is not intended to be, and should not be, used to replace specific advice relating to individual situations and we do not offer, and this should not be seen as, legal, accounting or tax advice. If you intend to take any action or make any decision on the basis of the content of this publication you should first seek specific advice from an appropriate professional. Some of the information in this publication may be compiled from third party sources we consider to be reliable, however we do not guarantee and are not responsible for the accuracy of such. The views expressed are not necessarily those of Willis Towers Watson.

About Willis Towers Watson

Willis Towers Watson (NASDAQ: WLTW) is a leading global advisory, broking and solutions company that helps clients around the world turn risk into a path for growth. With roots dating to 1828, Willis Towers Watson has 45,000 employees serving more than 140 countries and markets. We design and deliver solutions that manage risk, optimize benefits, cultivate talent, and expand the power of capital to protect and strengthen institutions and individuals. Our unique perspective allows us to see the critical intersections between talent, assets and ideas – the dynamic formula that drives business performance. Together, we unlock potential. Learn more at willistowerswatson.com.

Willis Limited, Registered number: 181116 England and Wales.
Registered address: 51 Lime Street, London, EC3M 7DQ.
A Lloyd's Broker. Authorised and regulated by the Financial Conduct Authority for its general insurance mediation activities only.

willistowerswatson.com/social-media

Copyright © 2020 Willis Towers Watson. All rights reserved.
WTW456603/06/2020/FPS1128

willistowerswatson.com

Willis Towers Watson