Marsh

Cyber Claims Snippets

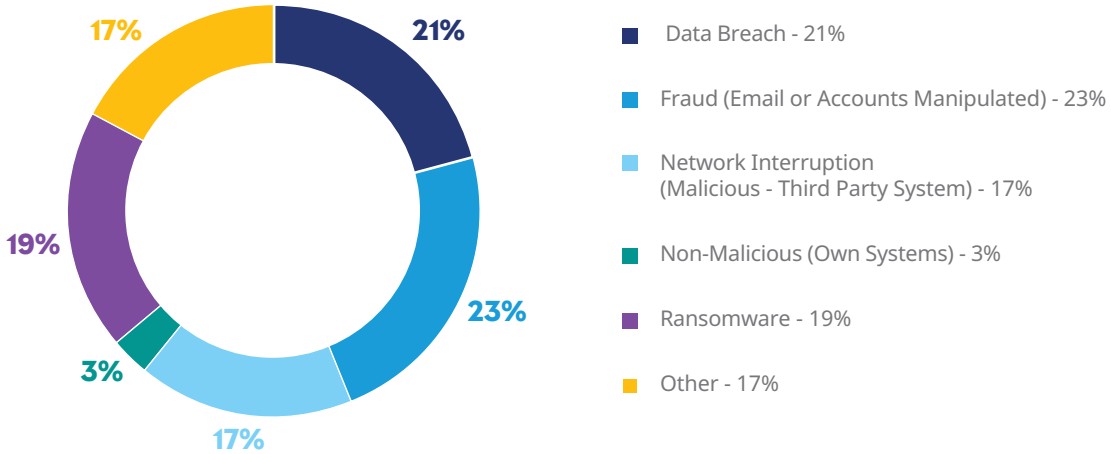
Second Half of 2021 in Review

Data breaches continued to dominate the headlines in the second half of 2021. Organisations that hold large amounts of confidential and sensitive information are a target for cyber criminals, as they recognise the attractiveness of selling stolen data on the dark web for a significant financial gain. Compared to the previous six months, the increase in severity of cyber claims were much more significant, whilst claims frequency only increased slightly. This snapshot of the second half of 2021 aims to highlight the cyber claims statistics and trends seen here at Marsh Pacific.

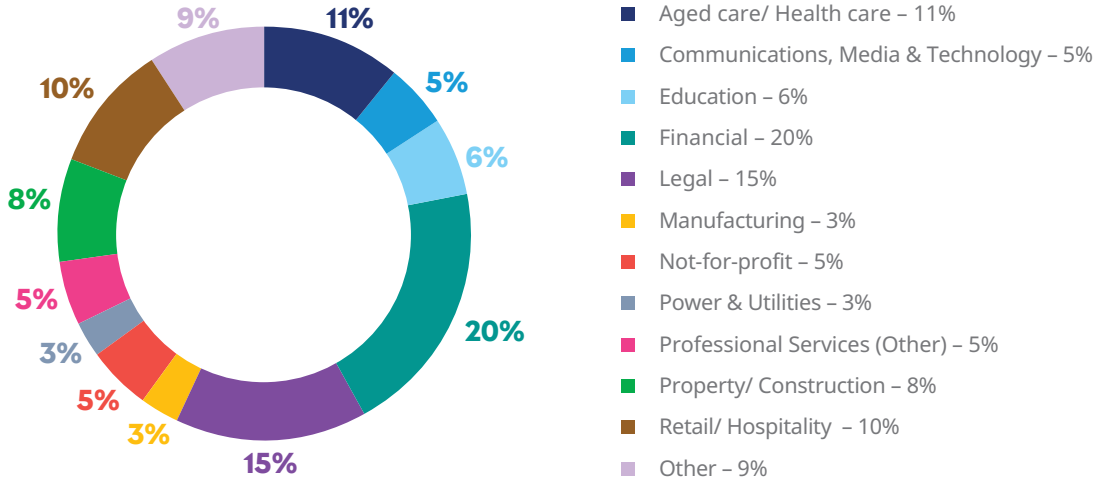
Marsh Pacific Claims Statistics

Summary of insights

- There was a 10% increase in the number of claims notified to insurers between 1 July 2021 – 31 December 2021, compared to the previous six months.
- Fraud (email or accounts manipulated), data breach and ransomware attacks continued to make up majority of the matters. This was followed closely by network interruption (malicious - third party system) claims.
- Similar to the first half of 2021, financial and legal were the top industries affected by cyber incidents.
- Business Email Compromise remains a popular method, as we have seen cyber criminals indiscriminately targeting all industries with this type of phishing attack.
- Dominating headlines locally were high profile cyber incidents such as the zero-day vulnerability known as Log4jshell and ransomware attack(s) targeting HR technology vendors Frontier and Kronos. We saw notifications come through as a consequence of these incidents, particularly with the latter – emphasising greater consideration needs to be given to supply chain risks.

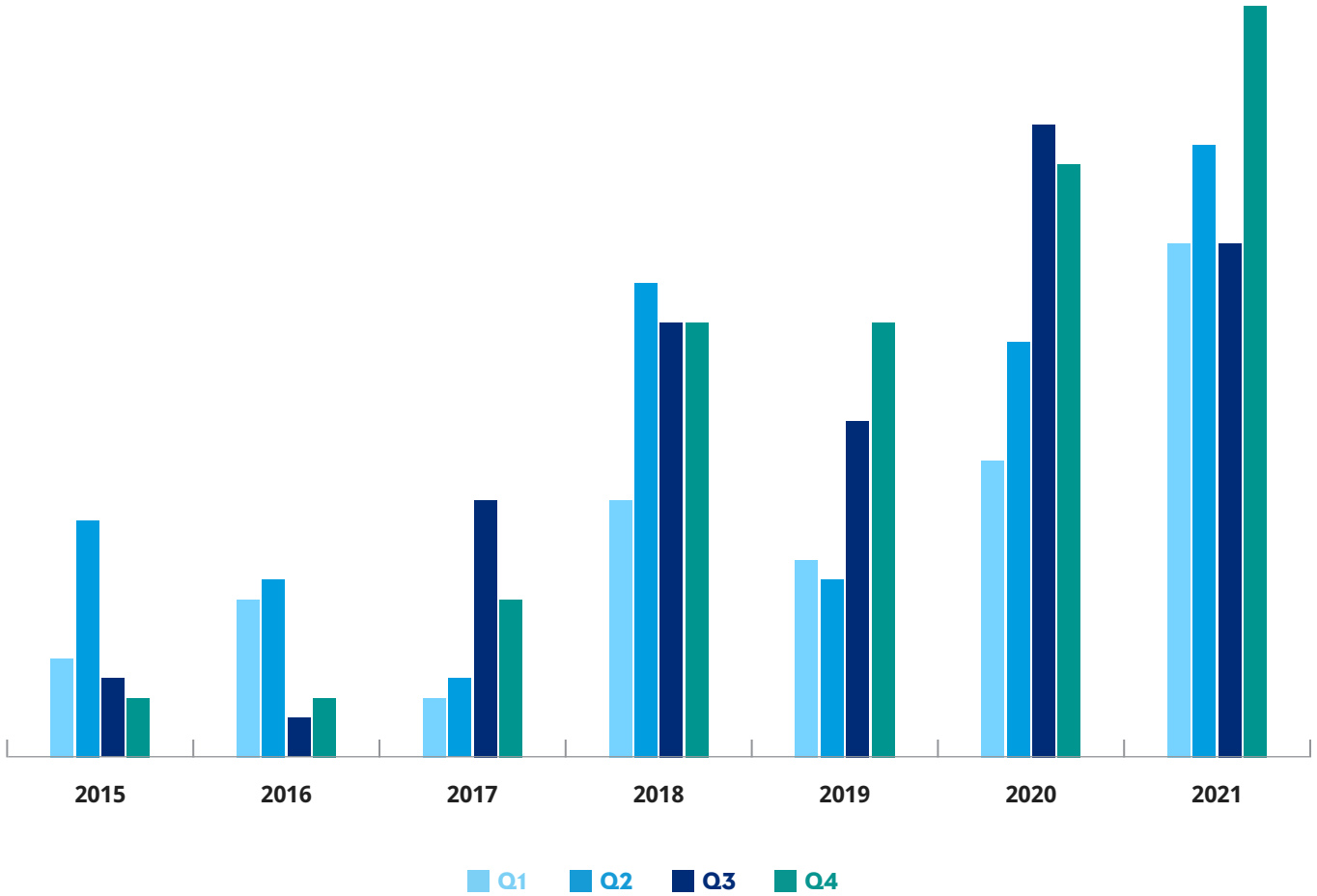


Incidents by Claim Type



Incidents by Profession

Graphs showing claims notified to insurers between 1 July 2021 – 31 December 2021



Proportion of Claims by Quarter

Graphs showing claims notified to insurers between 1 July 2021 – 31 December 2021

Claims Trends

Data Breaches

Data breaches have already proven to be a reoccurring theme for Australian and New Zealand businesses and we expect this to only get worse into 2022. The value cyber criminals place on the data they have stolen, is reflected in the claims trends we have been witnessing throughout the second half of 2021. For example, with ransomware attacks, 'double extortion' tactics remain popular with cyber criminals, where they are not only encrypting sensitive data, but also accessing and exfiltrating the data; using it as leverage to compel businesses into engaging and ultimately paying the ransom demand. In some instances cyber criminals are taking it a step further by utilising stolen data from organisations to threaten internal executives, external clients and third parties to further leverage a ransom.

Business Email Compromise

The COVID-19 pandemic saw drastic changes in the way we do business. Conversations turned digital and technology replaced paper. Cyber criminals also saw the pandemic as an opportunity to exploit the vulnerabilities caused by these factors. Accordingly, it comes as no surprise that Business Email Compromise **('BEC')** remains prevalent. Since most organisations are heavily dependent upon email as their primary method of communication between customers and vendors, cyber criminals are commonly seeking ways to abuse the trust that has been built. BEC scams often begin with compromising a work email using stolen credentials, phishing or brute force attacks (a form of cyber-attack that relies on guessing possible combinations of a targeted password until the correct password is discovered).[1] Once a cyber-criminal has email access they impersonate the trusted party and attempt to scam money or goods from third parties. As the fraudulent emails are sent from a legitimate email address they are able to slip through the spam filters and their authenticity is rarely questioned. BEC scams are commonly associated with invoice fraud as criminals aim to swindle large sums of money from victims quickly before a compromise is reported.

Technology Supply Chain Attacks

A number of large scale ransomware attacks targeting supply chain vendors were reported last year including third party service providers like Kronos and Frontier Software who provide payroll solutions to clients. As a consequence, Australian organisations utilising these service providers were impacted. The targeting of outsourced service providers continues to be popular with cyber criminals. This is due to the large volumes of sensitive customer data managed and the privileged access into their customer's systems held. Additionally, the impact of a business interruption is magnified considerably due to the sheer number of businesses that are dependent on these vendors for their own operations. The Australian Cyber Security Centre (ACSC) has emphasised the point that organisations need to plan for incident response in the event of a software supply chain compromise.[2]

1| https://www.forcepoint.com/cyber-edu/brute-force-attack
2| https://www.cyber.gov.au/acsc/view-all-content/reports-and-statistics/acsc-annual-cyber-threat-report-2020-21

Legal and Regulatory Update

Throughout the second half of 2021, we saw the tightening of regulations, expectations and accountabilities regarding cyber security. The following list highlights the major changes from a legal and regulatory perspective.

PART I: Regulatory Bodies Zooming in on Cyber Security

Office of the Australian Information Commissioner (OAIC):

The OAIC found that Uber Technologies Inc. violated the privacy of an estimated 1.2 million Australians. The findings include Uber's failure to investigate and disclose a data breach from 2016 in a timely manner. It was noted that Uber did not conduct a full assessment of the breach until almost a year after the attack in November 2017. As a result, the OAIC ordered Uber to prepare a data retention and destruction policy, information security program and incident response plan within three months, as well as appoint an independent expert to review the actions and report to OAIC within five months.

"Australians need assurance that they are protected by the Privacy Act when they provide personal information to a company, even if it is transferred overseas within the corporate group." ***– Information and Privacy Commissioner, Angelene Falk***

Australian Securities and Investments Commission (ASIC):

In December 2021, ASIC released Report 716 Cyber resilience of firms in Australia's financial markets: 2020–21.[3] The report found that there has been a small but steady improvement in the cyber resilience of firms operating in Australia's financial markets. In particular, cyber resilience of small-to-medium enterprises (SMEs) has improved, closing the gap between large firms and SMEs.

"The COVID-19 pandemic has increased opportunities for threat actors to target remote workers, and access remote infrastructure and supply chains critical to the delivery of products and services. However, the response from firms has been robust." ***– ASIC Commissioner, Cathie Armour***

Australian Competition and Consumer Commission (ACCC):

In response to the ACCC's Digital Platforms Inquiry Report of June 2019, Attorney-General's Department released an Exposure Draft of the Privacy Legislation Amendment (Enhancing Online Privacy and Other Measures) Bill 2021 to amend the Privacy Act 1988 (Cth). This Bill proposes to establish a framework to develop, implement and enforce a binding online privacy code for social media and certain other platforms. It also proposed to update the OAIC's enforcement powers, as well as increase current penalty provisions and to clarify the extraterritorial scope under the Privacy Act.

PART II: Australian Legislative Reforms

Ransomware Payments Bill 2021

The Ransomware Payments Bill 2021 (Cth) was tabled in June 2021, which sought to impose mandatory notification obligations to the Australian Cyber Security Centre (ACSC) on organisations that make a ransomware payment. If passed, key impacted organisations include Commonwealth and State Government agencies, and companies that turnover more than $10 million annually. Any non-compliance may result in potential fines up to $222,000.

"Mandatory notification; it's no silver bullet. It won't solve this problem, but it's the foundation stone for all the other actions we want to take."
– Shadow Assistant Minister for Cyber Security, Tim Watts

New Zealand Consumer Data Right

On 5 July 2021, the NZ Government decided to implement a new legislative framework for a consumer data right. This will allow consumers to securely share data that is held about them with trusted third parties, using standardised data formats and interfaces. In early 2022, the Government will make further decisions about the implementation of the Consumer Data Right **('CDR')**. This will include decisions on which institutions have a role in implementation and developing rules and standards, and measures for enforcing the consumer data right. The Government will also consider which sectors should be assessed first for the potential application of the CDR.

3| https://asic.gov.au/about-asic/news-centre/find-a-media-release/2021-releases/21-331mr-asic-reports-on-cyber-resilience-assessments-of-financial-markets-firms/

Ransomware Action Plan

In October 2021, the government introduced the Ransomware Action Plan which provides a blueprint for strengthening cyber security and provides organisation with advice in preparing for and responding to cyber attacks. Some considerations include making the reporting of ransomware incidents to the Australia Government mandatory for entities with annual revenue of more than $10 million. It further intends to introduce new offences for perpetrating ransomware.

The Crimes Legislation Amendment (Ransomware Action Plan) Bill 2022 (Cth) has since been tabled, introducing new standalone offence for all forms of cyber extortion with increased maximum penalty of 10 years' imprisonment, and 25 years for cybercriminals seeking to target critical infrastructure. It also provides law enforcement with great power to monitor and freeze cybercriminals' ill-gotten gains, as well as seizing digital assets (including cryptocurrency).

"This Bill gives Australian law enforcement agencies the legal tools and capabilities they need to pursue and prosecute ransomware gangs and the pervasive threat of ransomware attacks on Australia and Australians."
– Minster for Home Affairs, The Hon Karen Andrews MP[4]

Security Legislation Amendment (Critical Infrastructure) Act 2021 (Cth)

In December 2021, the Security Legislation Amendment (Critical Infrastructure) Bill 2020 (Cth) received royal assent. The Security Legislation Amendment (Critical Infrastructure) Act 2021 (Cth) has expanded the 'critical infrastructure' operation from 4 to 11 additional sector coverage, with flow-on implications for mandatory cyber security incident reporting. The Act also requires certain entities to maintain a register of critical infrastructure assets containing specified information.

In particular, entities which are captured under the legislation must now adhere to the following reporting obligations:

- Critical cyber security incidents must be reported within 12 hours of the entity becoming aware of the event. An event will be considered critical where it has a "significant impact."
- Other cyber security incidents must be reported within 72 hours if they have a "relevant impact" on the availability, integrity, reliability, or confidentiality of the critical infrastructure asset.

4| https://www.homeaffairs.gov.au/cyber-security-subsite/files/ransomware-action-plan.pdf

Food For Thought

As the frequency of ransomware attacks on Australian and New Zealand businesses continues to increase, a common question that arises is whether or not to pay a ransom demand.

As a starting point, law enforcement agencies generally advise organisations against paying ransoms. However, the Australian Financial Review reported in October 2021 about one in three companies in Australia that are the subject of ransomware attacks pay up, with the average size of the payment $1.25 million, often in Bitcoin or some other form of cryptocurrency.[5]

In recognising that there may be unique circumstances where payment is necessary, prudent organisations should arm themselves with information around the potential implications of paying a ransom. We recommend that organisations discuss in advance when, how and under what conditions your organisation would make payment. Organisations should incorporate that decision-making framework into broader plans and policies governing cyber and ransomware related risk.

Here are a list of potential considerations when deciding whether to pay or not to pay a ransom:

5| https://www.afr.com/technology/why-companies-will-ignore-the-government-and-pay-hackers-ransoms-20211015-p5909v

Reasons for paying a ransom	Reasons against paying a ransom
If backups have been configured improperly, have not been tested to restore systems or have been compromised or infected with malware.	Ransom demands can be extremely expensive with the highest ransom demand of 2021 reaching over US$40m.
When the data stolen by cyber criminals is extremely critical/sensitive in nature and will negatively impact the business and/or third party if stolen/leaked.	There is a chance that decryption key provided by hackers may not work or hackers may not provide a decryption key despite receiving payment.
When encrypted data results in business interruption recovery may be extremely important and time critical due to either the nature of the organisation or the significant loss of revenue and increased cost of working that is being incurred while systems are unavailable.	There is no guarantee that cyber criminals will delete all stolen data and could still chose to sell or publish exfiltrated data on the dark web.
In many situations the total cost of data recovery and network remediation without a decryption key would be far greater than just paying a ransom demand.	Paying a ransom may arguably give hackers more incentive and support to conduct ransomware attacks in the future, further perpetuating the cycle of ransomware attacks.

Exclusive Q&A with the Founder of Coveware

Bill Siegel founded Coveware in 2018 because despite ransomware becoming a major problem, there was zero high quality data available. One of Coveware's core principles has always been to aggregate as much high quality data about these incidents. Many experts believe that ransomware will never disappear, but Bill is of the view that we can contribute to dramatically curtailing the prevalence of this risk. We spoke with Bill to obtain an insight into what life of a ransomware negotiator is like, better understand the challenges pertaining his role and get his thoughts on the impact that the regulation of cryptocurrency may have on ransomware attacks.

What does a day in the life of a ransomware negotiator look like?

It is probably not as glamorous as one might think. It is a lot of time on the phone talking with victims of cyberattacks, collecting and aggregating information necessary to help us develop a cohesive recovery strategy, and relentlessly keeping very close track of all the details of the matter. Our team also spends a lot of time workshopping strategies and scenarios internally so that we all benefit from the combined and diverse experience of the entire team.

Do you have a set script to follow when you negotiate with the cybercriminal? If no, what factors are you guided by in order to determine the best negotiation strategy to adopt?

Every matter is unique, as every victim has a unique set of circumstances, and the strategy needs to fit those circumstances. These factors principally involve the urgency of the situation and what the client actually needs to achieve. This is then matched against what our data shows as the statistical probability of achieving those deliverables.

What is the general process when paying a ransom in cryptocurrency and how does Coveware help to facilitate the transaction?

There is probably a bit too much detail for this interview, but most of the process involves our sanctions compliance process and ensuring that all the necessary data has been collected and check boxes checked.

Due diligence procedures are performed to minimise the chance that the cybercriminal will renege on the agreement, the procedure of which varies depending on the specific cybercriminal or group as they all have their own unique set of risks.

How easy is it to attribute a ransomware attack to a particular threat actor?

The variant of ransomware is normally straightforward to attribute. WHO the person or group is can be very fluid though, and that is the trickiest part.

What is the most challenging part about your job?

Every aspect is a challenge, but I truly enjoy it. Even during the most stressful negotiations, like hospital cases where patients may be at risk, or 3 hour management table top training sessions. It feels good to help people and companies in need, and it feels good to know that the proactive training we provide is helping organisations avoid these incidents.

Do you see the trend towards regulation of cryptocurrency having an impact on the ransomware landscape?

Of course. Regulators have the power to effectively prohibit a ransom payment by proxy, even if there is no specific law that states “No company shall pay a ransom…” This would be pretty short cited regulation though as ransomware’s success does not depend on cryptocurrency. This sentiment has been shared by law enforcement agencies as well (if you are curious see the HSGAC testimony from the summer of 2021). As long as organisations are penetrable in a cost effective manner, threat actors will continue to break in and wreak havoc. The method through which they try to extort and monetize the attack would just shift to something else in the absence of cryptocurrency. That shift may impact the profitability of cyber extortion, as laundering the proceeds would become more expensive, but it would be very naive to think that regulating or trying to ban cryptocurrencies will have any impact on how these threat actors operate.

And finally if you are at a BBQ and someone asks you what do you do for a job, what do you say?

Hah, it is too complicated to explain and I’m pretty reserved, so I generally just say I work in cybersecurity, and change the topic.

Cyber Fun Facts

DID YOU KNOW?

The most common password in Australia is 123456 which can be brute-forced[6] by computer hack instantaneously.[7]

Received a dodgy shopping text recently? Since August 2021 there has been over 16,000 reports of Flubot scam text messages to Scamwatch.[8] These phishing texts are targeting Australians in an attempt to infect their mobile device with malware, gain banking details and steal personal information.

Deep-faked voices are now being used to impersonate executives for business email compromise scams in an attempt to steal funds from organisations. In one report, a voice deep-fake was used to scam a UK energy company out of USD$243,000 by impersonating the voice of their CEO.[9]

The Darkweb's largest forum for selling stolen credit and debit cards 'UniCC' announced they are shutting down operations after pocketing over US$350m in cryptocurrency since opening in 2013.

In a surprising twist of events, several members of the notorious 'Revil ransomware gang' were arrested by the Russian Federal Security Service (FSB) and neutralised their operations.[10]

6| https://www.varonis.com/blog/brute-force-attack

7| https://australiancybersecuritymagazine.com.au/200-most-common-passwords-of-2021-in-australia/

8| https://www.scamwatch.gov.au/news-alerts/missed-delivery-call-or-voicemail-flubot-scams#:~:text=Since%20August%202021%2C%20many%20Australians,missed%20calls%2C%20voicemails%20or%20deliveries.&text=However%2C%20the%20message%20is%20fake,actually%20malicious%20software%20called%20Flubot.

9| https://www.wsj.com/articles/fraudsters-use-ai-to-mimic-ceos-voice-in-unusual-cybercrime-case-11567157402

10| https://www.wired.com/story/russia-revil-ransomware-arrests-ukraine/

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 mmc.com, follow us on LinkedIn and Twitter or subscribe to BRINK.