Marsh

July 2021

# Cyber Claims Snippets

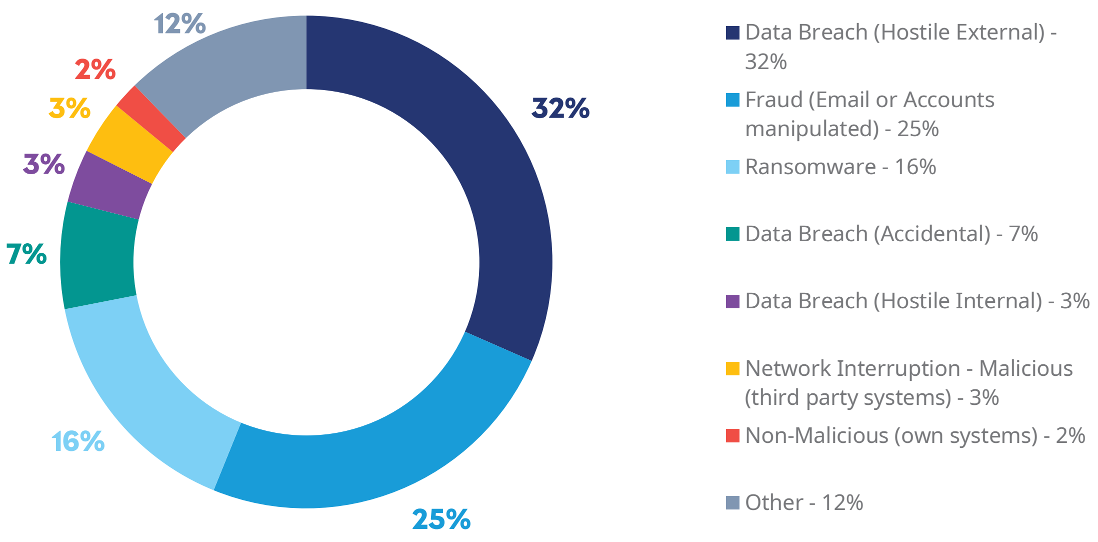
First Half of 2021 in Review

Compared to the same time last year, cyber attacks have increased both in terms of frequency and the level of sophistication. As cyber threats are constantly evolving, law reforms are being considered in an attempt to keep on top of the incessant changes in the cyber landscape. This snapshot of the first half of 2021 aims to highlight the cyber claims statistics and trends we are seeing here at Marsh Pacific.

# Marsh Pacific Claims Statistics

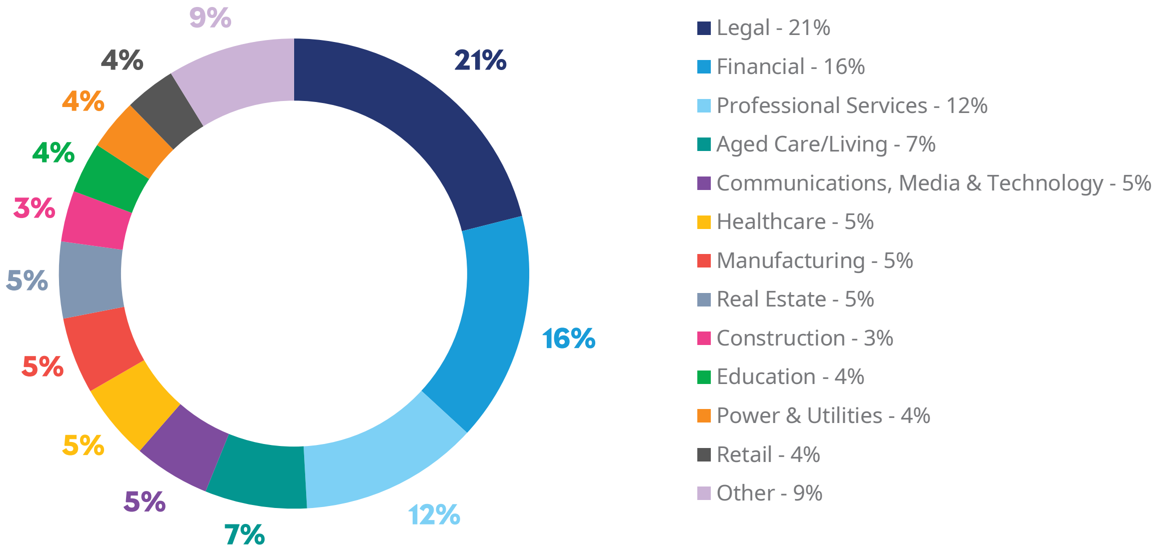
## Summary of insights

- Cyber claims have increased by nearly 50% compared to the same time last year.
- Ransomware attacks, data breaches (hostile external) and fraud (emails or accounts manipulated) made up majority of the matters.
- Business Email Compromises (fraud) continue to be a significant threat to organisations especially for SMEs.
- The legal, financial and professional services industry is becoming an increasingly attractive target for cyber criminals, with a majority of the ransomware attacks arising from incidents involving law firms.
- Incident Response Expenses and Business Interruption Loss are two aspects of the policy commonly triggered.



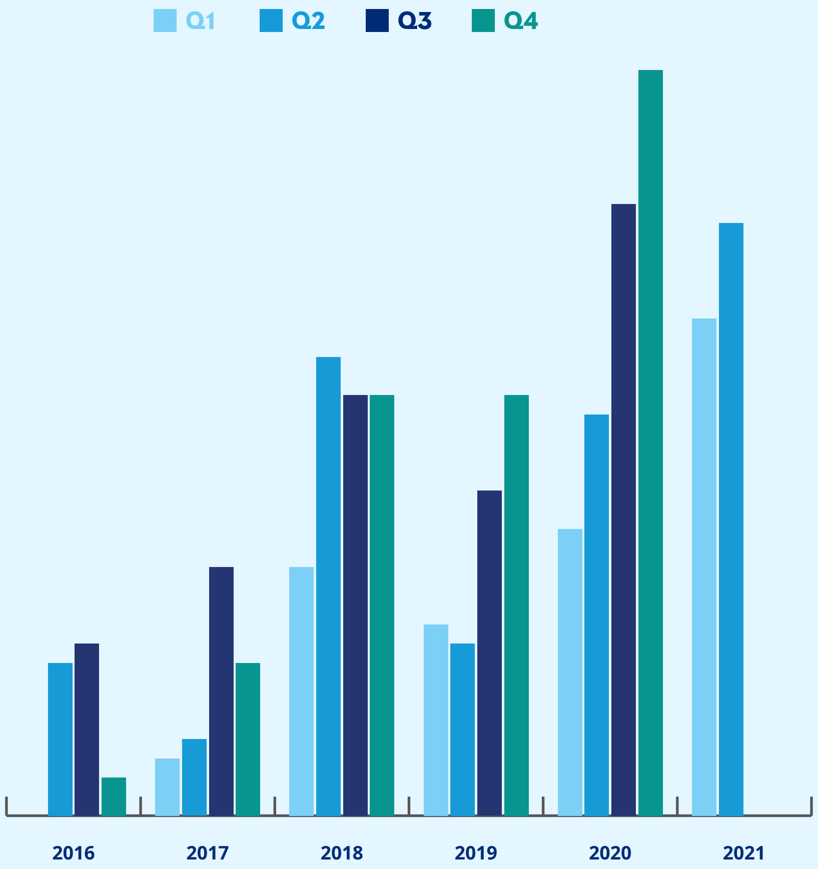
## Incidents by Claim Type

This data is based on claims notified to insurers for the period 1 January 2021 to 30 June 2021



## Incidents by Profession

This data is based on claims notified to insurers for the period 1 January 2021 to 30 June 2021



## Proportion of Claims by Quarter

This data is based on claims notified to insurers for the period 1 January 2021 to 30 June 2021

# Claims Trends

## Ransomware

Ransomware continues to be a major threat to Australian and New Zealand organisations of all sizes, industries and revenues. Double extortion techniques (where cyber criminals encrypt and threaten the publication of data they have exfiltrated) have become standard practice across the majority of ransomware attacks we are seeing. Some are now moving to include triple layer extortion which refers to the additional vectors of attack used to pressure victims to pay the ransom. Examples may include cyber criminals launching Distributed Denial of Service (DDoS) attacks against organisations to completely cripple their network; or utilising the data stolen from organisations to threaten internal executives, external clients and third parties that are also affected by the breach to further leverage a ransom.

## Technology Supply Chain Risk

Throughout the first half of 2021, multiple high profile global technology breaches resulting from software vulnerabilities, were discovered. These included the likes of Microsoft Exchange, Solarwinds, Accellion and Kaseya. As a consequence, Australian organisations utilising these softwares were impacted. It comes as no surprise that technology supply chain attacks have proven to be popular with cyber criminals, as these third parties often manage a large pool of sensitive client data, supply foundational software platforms, or have privileged access to their customer's systems. The Australian Cyber Security Centre (ACSC) has further emphasised this point, stating that managed service providers are being continuously targeted by cybercriminals.[1]

## Critical Infrastructure

Australian and New Zealand critical infrastructures have a significant reliance upon technology driven processes, providing hackers with a potential vulnerability to abuse. The targeting of these critical assets has become commonplace as nation states and other cyber criminals understand the potential disruption and widespread chaos that a shutdown can cause. This is evident in the ransomware attack on JBS Foods which saw the shutdown of its US and Australian operations during the first week of June 2021. The company subsequently paid AUD$14 million to the criminal gang to recover control of its critical infrastructure and mitigate data exfiltration[2].

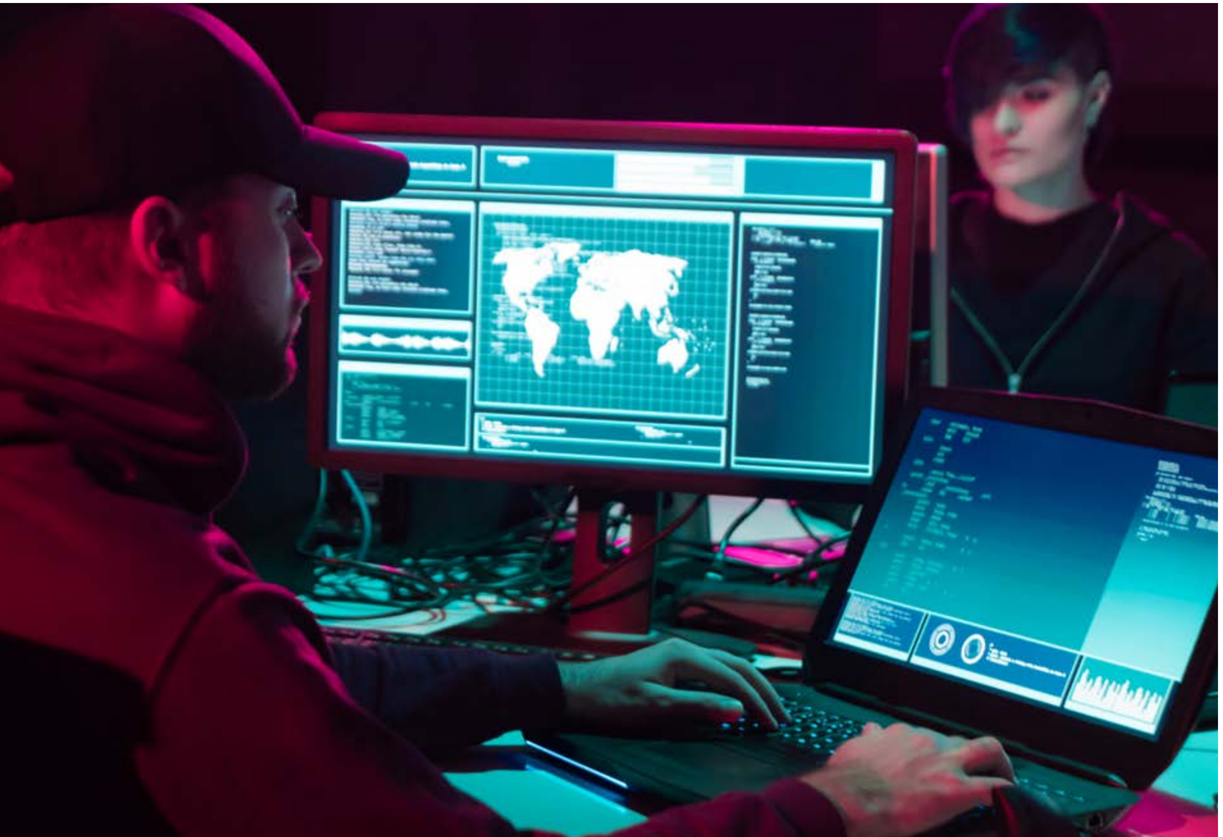
[1] © Commonwealth of Australia 2020; https://www.cyber.gov.au/acsc/view-all-content/news/head-acsc-address-aisa-cyber-conference-2021

[2] https://jbsfoodsgroup.com/articles/jbs-usa-cyberattack-media-statement-june-9

# Food For Thought:

## SHOULD RANSOMWARE PAYMENTS BE MADE ILLEGAL?

As ransomware is considered a top cyber security threat by most organisations, this has driven renewed interest in the debate as to whether ransomware payments should be banned. What do you think?



| For | Against |
|---|---|
| Prevents ransom payments from funding cyber criminals, terrorists and the ransomware economy, discouraging future attacks. | Limits the recovery options available to organisations and forces them to rely more heavily upon backups. Backups are likely to become more targeted. |
| As there is no guarantee that cyber criminals will provide a decryption key, could potentially prevent companies from wasting money. | Being unable to pay a ransom could further threaten the survival of the company as attacks could instead move to selling stolen personally identifiable information of its clients and customers instead. |
| No certainty that hackers will delete or return stolen data when a ransom is paid and could potentially be a wasteful expense. | A single government banning ransom payments is unlikely to solve a global problem as hackers will switch to target different countries or overseas entities. |
| Ensures that organisations cannot intentionally/unintentionally break trade sanctions when paying a ransom. | Criminalising ransom payments will result in a lack of threat reporting and drive an underground crime trade, making it difficult to enforce non-payment. |

# Legal and Regulatory Update

**PART I: Regulators** are proactively honing in on cyber security compliance and utilising their power to secure enforcement outcomes pertaining to data breaches.

### Office of the Australian Information Commissioner (OAIC):

OAIC's ruling which mandated Department of Home Affairs to compensate over 9,000 individuals after their details (including names, dates of birth, citizenship status, location, boat arrival details and the period individuals had spent in immigration detention) were inadvertently released on their website in February 2014. Compensation ranged from $500 to more than $20,000 which would be assessed on a case-by-case basis.

*"This matter is the first representative action where we have found compensation for non economic loss payable to individuals affected by a data breach." – Australian Information Commissioner, Angelene Falk*[3]

### Australian Securities and Investments Commission (ASIC):

ASIC relied upon the *Corporations Act 2001 (Cth)* to commence proceedings against RI Advice Group (an Australian Financial Services licence holder focused on retirement advice) in August 2020 for failing to have adequate cyber security systems. Proceedings are currently ongoing and the matter has been tentatively listed for trial commencing 29 November 2021.

*"We are assisting our regulated population in their efforts to improve cyber resilience. And we've shown that we will litigate when necessary." – ASIC Commissioner, Sean Hughes*[4]

### Australian Competition and Consumer Commission (ACCC):

In ACCC v Google LLC & Google Australia Pty Ltd, the Federal Court ruled on 16 April 2021 that Google had misled Android users as to how much of their personal location data was being collected. The ACCC is seeking declarations, pecuniary penalties, publication orders, and compliance orders, which will be determined at a later date.[5]

*"Today's decision is an importance step to make sure digital platforms are up front with consumers about what is happening with their data and what they can do to protect it." – ACCC Chair Rod Sims*[6]

### Office of the Privacy Commissioner – New Zealand (OPC):

Since the *Privacy Act 2020 (NZ)* came into force in December 2020, early indications appear to suggest that mandatory breach reporting regulations are working.

The Office of the Privacy Commissioner has revealed that 76 'serious' privacy breaches have been reported between 1 December 2020 and 31 March 2021. This is a 97% increase in privacy breach notifications in the first four months when compared to the previous six months.[7]

*"The law change means that if an organisation suffers a serious privacy breach, it should tell my Office as soon as practicable after becoming aware of the breach." – NZ Privacy Commissioner, John Edwards*[8]

**PART II: Australian Legislative reforms** are being considered to better protect businesses and individuals from cyber threats.

The *Ransomware Payment Bill 2021 (Cth)* aims to impose a "ransomware payment notification scheme" whereby government agencies and business that turnover more than AUD$10m will be required to notify the Australia Cyber Security Centre before paying a ransom.

The *Privacy and Personal Information Protection Amendment Bill 2021 (NSW)* aims to strengthen privacy protection in NSW and proposes to:

- Improve the effectiveness of privacy enforcement, including increased penalties for serious or repeated privacy breaches; and
- Establish a mandatory reporting of data breaches which are likely to result in serious harm.

The *Security Legislation Amendment (Critical Infrastructure) Bill 2020 (Cth)* seeks to expand scope to include critical infrastructure entities in a wider range of sectors. The reforms will introduce enhanced cyber security obligations and government assistance to respond to cyber attacks in the event of a cyber emergency.

[3] https://www.oaic.gov.au/updates/news-and-media/information-commissioner-orders-compensation-payable-by-home-affairs-for-breaching-detainees-privacy/

[4] https://asic.gov.au/about-asic/news-centre/speeches/conversation-with-asic-afia-risk-summit/

[5] © Commonwealth of Australia 2020

[6] https://www.accc.gov.au/media-release/google-misled-consumers-about-the-collection-and-use-of-location-data

[7] https://www.privacy.org.nz/assets/Privacy-Week/Serious-breach-notification-infographic.pdf

[8] https://www.privacy.org.nz/publications/statements-media-releases/reported-privacy-breaches-double-after-new-privacy-act-takes-effect/

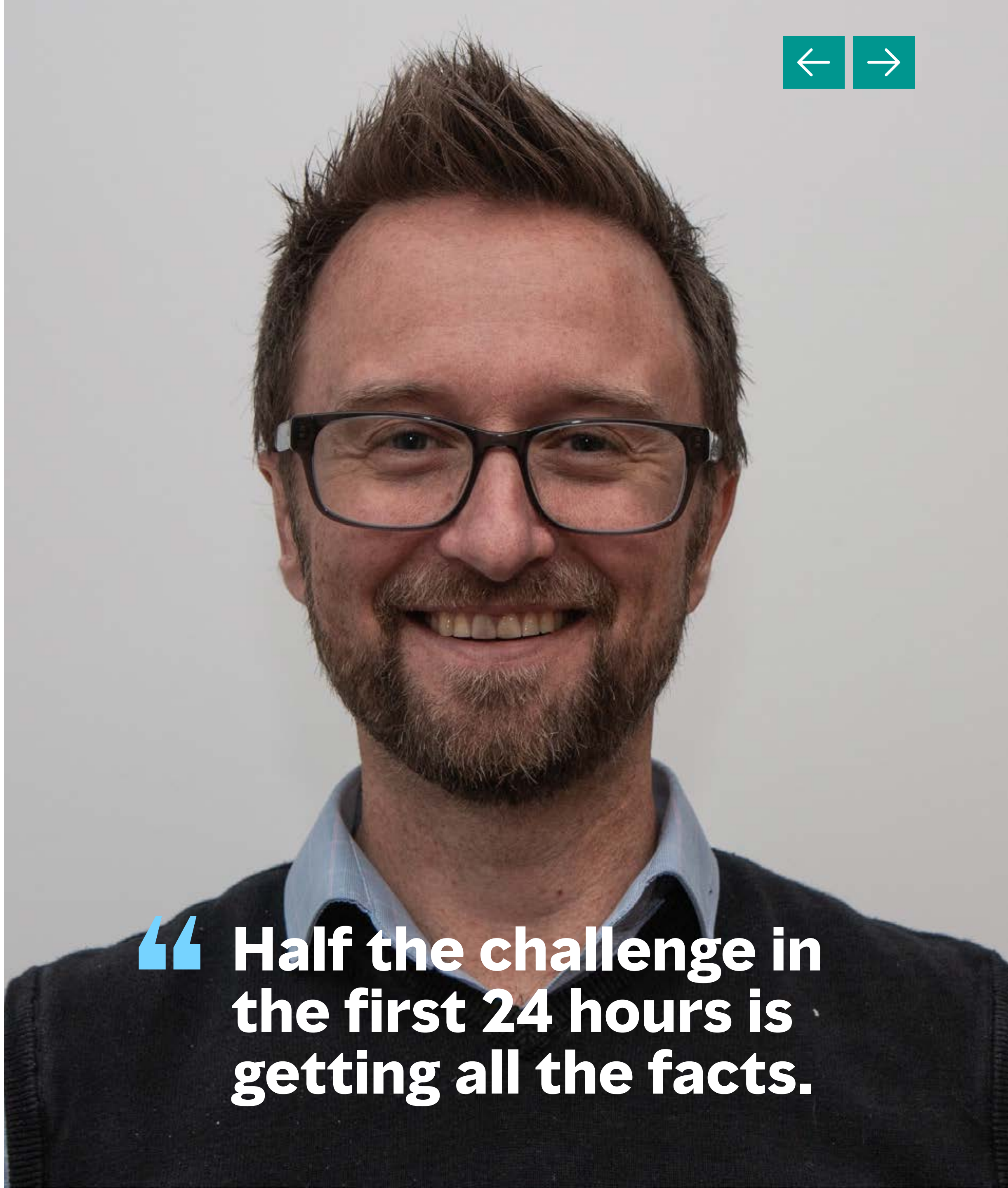
# Exclusive Q&A with the Founder of Insane Technologies

When David Rudduck founded Insane Technologies over two decades ago, his first matter involved reviewing the security of a superannuation administration company and trying to convince them not to use their name as their password (it was also their username). We spoke with David to learn how his job has since changed, his insight into Australia's cyber security practices and advice to organisations on building a culture of cyber security.

**Insane Technologies was acquired by CFC Underwriting in 2021 to form part of their Australian Response Team. As an incident response manager, you are now often the first point of contact when a cyber incident arises. Could you walk us through what usually happens within the first 24 hours of an incident?**

Cyber incidents start as computer problems. Someone comes in to do a job and finds the IT systems aren't working properly. They log a ticket with IT Support, who start investigating and then get to a point where they realise "oh snap, we've been hacked". After then it's panic.

Half the challenge in the first 24 hours is getting all the facts. Can we get an asset list? Who are the vendors involved? Can we get a kick off meeting started? Can we get access to any systems that are still running to start threat hunting? Do the backups work? What logging data is available?



> **"Half the challenge in the first 24 hours is getting all the facts.**

The biggest challenge is helping the business to get focus on the big-ticket items, look for work arounds for business continuity, and getting everyone onto the same page.

### There is no doubt that you have had a diverse career in the IT industry with an extensive range of both national and international experience. How do you think Australian cyber practices stack up on a global scale?

Compared to the USA and UK, we're at least 5 years behind, maybe 10. Compared to some of our greatest adversaries, we're nearly 20 years behind.

Many business owners don't consider "cyber" a risk to their business until they, their friends, or a business in their industry is affected. We need to be more proactive about our approach.

### What are some of the biggest mistakes you see companies making in relation to their security practices?

Many businesses struggle to implement good security controls when they get push back from staff and pull up the handbrake. Change management is a difficult thing, and a lot of the push back is usually due to a misunderstanding. Wrong or right, cyber security is deemed less important than user experience and "getting on with business".

Like Multi Factor Authentication. Just turn your MFA on already! Your boss isn't monitoring you through the authenticator application. Really!

### What is more difficult – preventing cyberattacks or recovering from one?

If we're talking commodity cyber criminals, definitely recovering from one. Most businesses take several months to properly recover from a major cyber incident.

### Clearly prevention is key here. What is the best way to build a culture of cyber security within organisations?

The board and senior management need to accept that they are 100% responsible for the cyber maturity of their business. They need to try to understand it better, at least from a risk and impact basis – as they are the ones that approve budgets for these things. Equally the IT and IS industry needs to get better at communicating in a language that the board can digest.

### Finally... Coffee or Tea?

Coffee. In a bucket. Please and thank you.

# Cyber Fun Facts:

## DID YOU KNOW?

A new cyber security incident is reported to the Australian Cyber Security Centre (ACSC) every 8 minutes.[9]

The infamous cybercriminal 'Joker' known for hosting stolen payment card transactions on their 'Joker Stash' dark web marketplace, announced their retirement in February 2021 with at least $2.1 Billion in Bitcoin.
**Who says crime doesn't pay?**

The notorious Ziggy ransomware gang announced in March 2021, that out of guilt and fear of law enforcement they would completely refund the extortion payments and offer free decryption keys to victims of their ransomware.

In June 2021 the FBI announced that they had seized over AU$3 million in Bitcoin of the ransom payment that the Colonial Pipeline had paid to Darkside.[10]
**Bitcoin may not be as untraceable and anonymous after all!**

Cyber criminals are organising themselves along the lines of drug cartels, employing increasingly sophisticated and targeted attack tactics, in an attempt to keep ahead of the cyber security advances.

[9] https://www.cyber.gov.au/acsc/view-all-content/news/head-acsc-address-aisa-cyber-conference-2021

[10] https://www.justice.gov/opa/pr/department-justice-seizes-23-million-cryptocurrency-paid-ransomware-extortionists-darkside

## About Marsh

Marsh is the world's leading insurance broker and risk advisor. With around 40,000 colleagues operating in more than 130 countries, Marsh serves commercial and individual clients with data-driven risk solutions and advisory services. Marsh is a business of Marsh McLennan (NYSE: MMC), the world's leading professional services firm in the areas of risk, strategy and people. With annual revenue over $18 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.

Disclaimer: Marsh Pty Ltd (ABN 86 004 651 512 AFS Licence No. 238983) arrange this insurance and are not the insurer. The information contained in this publication provides only a general overview of subjects covered, is not intended to be taken as advice regarding any individual situation and should not be relied upon as such. Insureds should consult their insurance and legal advisors regarding specific coverage issues. All insurance coverage is subject to the terms, conditions, and exclusions of the applicable individual policies. Marsh cannot provide any assurance that insurance can be obtained for any particular client or for any particular risk.

If this communication contains personal information we expect you to treat that information in accordance with the Australian Privacy Act 1988 (Cth) or equivalent. You must advise us if you cannot comply.