Deakin University

WTW Cyber & Technology

Benjamin Di Marco

September 2024

Benjamin Di Marco

WTW Cyber and Technology Risk Specialist

Ben has **over 15 years of experience specialising in cyber risk, privacy, technology law, financial insurance and dispute resolution**. He has acted in over 300 data breaches providing triage, privacy, strategic and claim support to companies.

Ben **leads WTW's Australia and New Zealand cyber and technology risk team** providing insurance, assessment, advisory and consulting services to domestic and international clients. Ben focuses on helping clients understand their exposure and developing responsive risk and resilience strategies matching business objectives and support needs.

Ben regularly conducts workshops for clients covering topics such as technology risk management, program placement, legal compliance, scenario tabletops, executive awareness, data and privacy governance, breach quantification, applied case studies, consensus-based action plans, third party risk, supply chain due diligence and insurance alignment.

Ben is also the Vice President of the Australasian Society of Computers and Law and sits on advisory bodies for the Australian Computer Society, Standards Australia, the Queensland Law Society and the NSW Law Society.

Benjamin Di Marco
Cyber and Technology Risk Specialist, ANZ
M +61 (0)478 312 988
Benjamin.DiMarco@willistowerswatson.com

What we will cover today

- **Cyber Insurance – Building Blocks**
- **Cyber Insurance – Exposures Alignment**
- **Submitted Questions**
- **Discussion**

Cyber Insurance: Building Blocks

Insurance Actions – Cyber Liability Insurance

What is it? What does it do?

Common First Party Coverages

First party provides coverage for the policyholder's own expenses arising from a cyber incident.

Cyber Insurance Coverage - Triage and Loss Mitigation

Breach Response Costs	Costs to triage and recover from a cyber or privacy breach, including expert costs for IT forensics, legal support, public relations expenses, notification, identity theft restoration, credit monitoring, and remediation expenses.

Cyber Insurance Coverage - Direct Financial Loss

Business Interruption	Income loss and extra expenses associated with your inability to prevent a disruption to your computer network caused by a cyber attack.
Data Restoration	Your costs to recreate or recollect data lost, stolen or corrupted due to your inability to prevent a cyber attack against your computer network.
Ransom Expenses	Your costs expended to comply with, mitigate, or to terminate a cyber extortion demand.
MSP Business Interruption	Income loss and extra expenses due to a network outage or disruption arising from a cyber attack against your third-party technology service provider.
Security System Failure	Unintentional or unplanned network outage or intrusion resulting from a security intrusion, or error, or omission in following a policy or procedure.

Common Third Party Coverages

Third party provides coverage for the policyholder's liabilities arising from a cyber incident e.g.

Cyber Insurance Coverage – Third Party Liability

Privacy and Data	Liability to impacted persons/stakeholders associated with your inability to protect personally identifiable information or the corporate confidential information of third parties.
Regulatory Liability	Request for information, civil investigative demand, or civil proceeding brought by or on behalf of any national, local or foreign governmental entity in such entity's regulatory or official capacity arising directly from a security or data breach. This includes regulatory fines and penalties incurred as a result of a cyber incident.
Network Security Liability	Liability costs associated with your inability to prevent a computer attack against your computer network.
Media Liability	Tort liability associated with content you create, distribute, or is created and distributed on your behalf.

What is cyber insurance?

Covers in more detail:

First Party coverages		
Insuring Clause	**Hypothetical scenario(s)**	**Coverage for**
Data Restoration costs	A malicious *third party* infects a policyholder's computer system with malware that destroys all customers data.	Coverage for fees and expenses to restore or recreate data held by the policyholder following a *system failure* or *security failure.*
Cyber Extortion (including Ransomware)	A malicious *third party* threatens to release a policyholder's customer data onto the *dark web,* unless the policyholder pays a ransom.	Extortion demands accompanied by threats to the policyholder's computer system triggering cover for: ▪ *ransom payments* ▪ expert fees for investigating threats and negotiating with criminals
Incident response costs	A data breach occurs, where a hacker gains access to a policyholder's computer systems and leaks customer information over the internet, leading to claims from their customers. You need assistance in respect of the following: ▪ Engage IT specialists to help identify the cause and extent of the impact of the incident, as well as to help resolve it (IT forensic costs) ▪ Understanding which regulators to notify (Legal services) ▪ Understanding how to notify affected customers and respond to claims (Legal services) ▪ Notify affected customers (Legal services) ▪ Provide Credit and ID theft protection monitoring to all affected customers ▪ Establishing call centre to handle enquiries/complaint ▪ How to communicate the message to the media (PR costs) This scenario could also apply if the breach occurs as a result of the negligent or deliberate act of an employee.	Direct costs for services (where appropriate) to respond to an actual or potential **network security**, **data breach** including: ▪ IT forensic costs ▪ Legal services ▪ Credit monitoring & ID theft protection services ▪ PR costs Often insurers provide an emergency telephone number that a member of the *Control Group* can call to obtain guidance in the event of an incident (performed by an incident response co-ordinator). This usually starts a process in which a summary of the incident is recorded and then the relevant experts are then engaged to assist the business in dealing with the incident.

What is cyber insurance?

Covers in more detail:

First Party coverages (continued)		
Insuring Clause	**Hypothetical scenario(s)**	**Coverage for**
Business interruption (non-physical damage)	***A) Security Failure*** A **malicious** actor performs a *Distributed Denial Of Service (DDOS)* attack on a policyholder's computer system, overwhelming it with traffic and resulting in the crashing of the website and preventing employees from using their computer workstations.	*Loss of net profit* as a result of an interruption to the policyholder's computer system following a *system failure* or *security failure,* in excess of a *waiting period.*
Business interruption (non-physical damage): *increased costs of working*	A policyholder suffers an interruption to their computer system as a result of a *system failure* or *security failure* and they need to employ temporary staff to make up for the loss of profits sustained over the period of severe interruption.	Additional costs a policyholder incurs in order to reduce the period of the interruption to aid continuation of normal operating procedures and reduce potential loss, examples include employee overtime or wages.
Third party business interruption (non-physical damage) **e.g. *IT Outsourced Service Provider***	**Security Failure** A policyholder's critical *IT Outsource Service Provider* gets hit by a *Distributed Denial of Service attack* causing an interruption to your service for 24 hours.	*Loss of net profit* as a result of an interruption to the policyholder's *IT Outsourced Service Provider's* computer system, following a *security failure.* A *security failure* is triggered by any intrusion of, or unauthorised access or use of your *IT Outsourced Service Provider's* computer system.

What is cyber insurance?

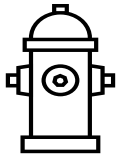
Covers in more detail:

Third party coverages		
Insuring Clause	**Hypothetical Scenario(s)**	**Coverage for**
Privacy and Data Liability	A data breach occurs on the policyholder's computer system, following a hacker gaining unauthorised access. The hacker leaks customer information over the internet, leading to legal proceedings from customers. This scenario could also apply if the breach occurs as a result of the negligent or deliberate act of an employee.	Liability claims from *third parties* (including *damages, claimants costs* and *defence costs*) as a result of an actual or alleged unauthorised disclosure or transmission of *personal information* or confidential *corporate information* held by a policyholder.
Regulatory Liability	The *Office of the Australian Information Commissioner* (OAIC) conducts a regulatory investigation into a policyholder's safeguarding of it's customers data, following a data breach.	*Defence costs* incurred in defending against data breach regulatory actions and resulting fines (where legally insurable) following a breach of data protection regulations.
Network Security Liability	An employee from the policyholder unwittingly sends an email containing a malicious attachment to an employee at Company B. The employee at Company B opens the attachment spreading malware throughout the computer system at Company B.	Liability for claims from *third parties* (including *damages, claimants costs* and *defence costs*) as a result of actual or alleged *security failure* such as transmitting a virus/malware or other malicious code etc.
Media Liability (Digital)	An employee of the policyholder posts a *defamatory* statement about a competitor on the policyholder's Facebook page.	Liability claims from *third parties* (including *damages, claimants costs* and *defence costs*) for *defamation,* unintentional intellectual property infringement, infringement or invasion of privacy arising from your website or *digital media activities.*

Cyber Insurance – Growing Pains?

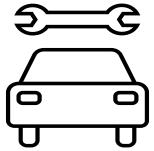
Cyber is an Emerging Insurance Solution

1676
First fire and property insurance policy was issued.

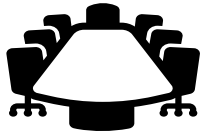


1706
First life insurance policy was issued.

1897
First automobile insurance policy was issued.



1930
First directors liability insurance policy was marketed.

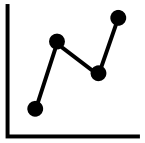


1995
First Cyber / Privacy Liability Policy issued

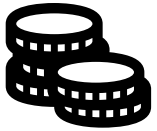
2002
First modular Cyber Wording issued

Current State

Limited Claims Data



Small Premium Pool



Evolving Response

Variance in Language

How does Insurance work in Practice?

Data breach is *discovered*
(and reported to management)

Client struggles with Immediate business need

Crisis environment and need to mitigate a myriad of risks from short term interruption, financial loss, long term business and reputational impacts and third party liability.

Support from Cyber Insurance

Breach response assistance:

Client calls a incident response **hotline number** shown on the cyber insurance policy, or other agreed proceed, to **co-ordinate** the following services to mitigate the impact of an incident (where relevant):

- IT Forensics
- Legal Services
- Notify / Monitor
- PR Costs

Policyholder

Present the insurer with the invoices for these services

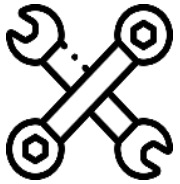
Insurer(s)

Pays for the costs incurred to deal with the incident

Cyber Insurance and Timelines

1

Notify incident to insurer

2

Vendors appointed

3

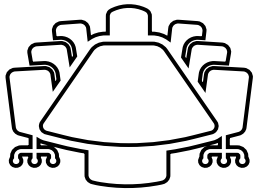
Investigation

4

Notification

5

Regulatory investigation


Business Interruption and Third Party Claims

Within 24 - 72 hours

- **Incident Identification and initial coordination**
- **Notification and establishment of rights under insurance policy.**
- **Initiation of incident response processes.**

Within 30 days

- **Grant of indemnity.**
- **Direct first party vendor costs and data restoration costs.**
- **Ransomware expenses.**

Long term – 6 months to 6 years

- **Resolution of regulatory investigations and actions.**
- **Addressing third party and stakeholder complaints.**
- **Privacy regulatory and civil liability actions.**
- **Defence and settlement of claims.**

Cyber Insurance and the rest of the Insurance Program?

Third Party Outcomes	Property	General Liability	Crime	Directors and Officers	Professional Indemnity	Dedicated Cyber Insurance
Third party legal proceedings: data protection liability						
Third party legal proceedings: network security liability						
Third party legal proceedings: digital media liability						
First Party Outcomes						
Regulatory investigation and defence costs						
Regulatory fines						**
Incident response costs						
Business interruption: loss of net profit (non- physical damage)						
Business interruption: increased costs of working (non - physical damage)						
Restoration of data and computer systems						
Ransom payments and expenses						
First party financial loss (theft of funds)						

Key not covered unlikely covered affirmatively covered

**** Cyber Liability Insurance will typically respond to privacy and data security related regulatory obligations.**

Insurance feedback – areas where organisations fall down

Backup Capabilities

Properly secured and reliable backups are a key control to reduce the severity of Ransomware losses.

Recommendations include:

- Encrypting backups.
- Multiple copies and backup sources, i.e., physically stored offsite and offline (3-2-1).
- Regular testing backups for data integrity and restorability.
- Regularly performing full and incremental backups of data.
- Identify realistic timeframes for full and partial restorations.
- MFA and strong access controls around backups.
- Regular testing of Incident Response / Business Continuity Plan including ransomware events and backup processes.

Legacy Assets

- Are there any unsupported or legacy systems used within the environment, including applications, software and hardware.
- What is the sensitivity of data stored within legacy systems?
- How critical are these legacy systems to the organisation?
- Has your organisation applied network segmentation (physical, logical etc.) to prevent unauthorised lateral movement into legacy assets?
- To what extent are third parties relied upon to operate or manage legacy assets?
- Have mitigating controls been put in place around legacy assets?

Multifactor Authentication

Holistic MFA rollout:

- Email
- Remote Network Access
- Privileged User Accounts
- Virtual Desktop Instances (VDI)
- Cloud resources including Office365
- Third Parties

Ransomware Preparedness

- Has your organisation determined contingencies and / or its formal response to a ransomware event?
- Do existing incident response and business continuity plan effectively account for ransomware crisis events?
- Has the organisation conducted exercises to test its response to ransomware?
- What controls exist for containment?

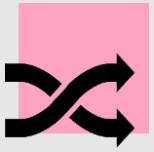
Cyber Insurance: Exposure Alignment

How do we respond to cyber incidents? Workstreams:

Incident Investigation

- IT and OT Investigation
- Logging and Data Preservation to Support Investigations
- Validating Back-Up Integrity and Failover Solutions
- Privacy and Data Security Risks Assessment
- Personal and Sensitive Data/Information Risk of Harm
- Preserving IT Infrastructure
- Staged Shutdown
- Counter-Party Risks

Recovery & Remediation



- Back-up Restoration
- Ransom Negotiation
- Ransom Payment Considerations
- Sanctions and Criminal Law Interplays
- Notifications Obligations
- Supply Chain Impacts
- Business Disruption and Operations
- Communications
- Credit Monitoring/ID Protection
- Stakeholder Complaints

Consequences

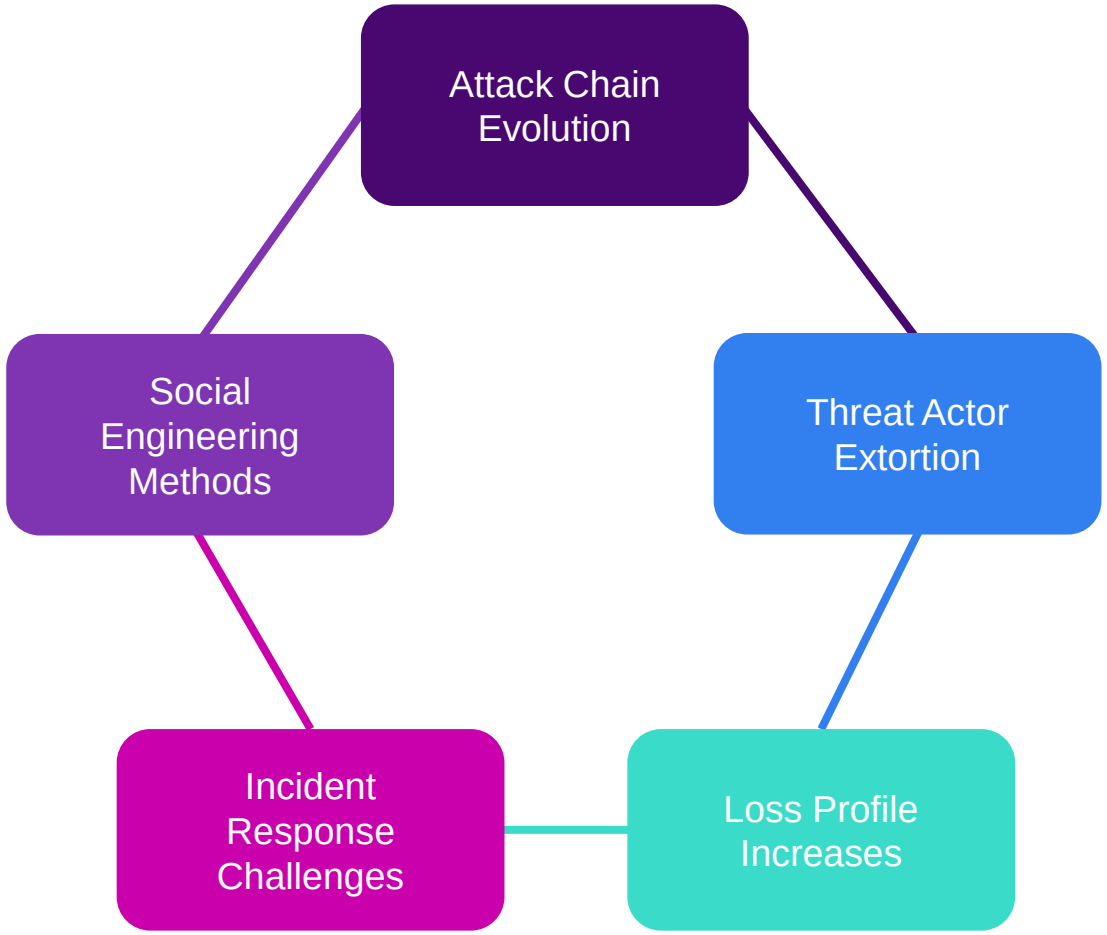
- Incident response costs.
- Fines, penalties and compliance.
- Business Interruption
- Exfiltration and data loss (financial harm, impairment, sensitivity, IP).
- Malicious actor engagement.
- Fraud risks.
- Double and triple extortion.
- Reputational harm.
- Stakeholder management.
- Regulatory actions.
- Litigation / class actions

Consequences - losses that follow a cyber incident?

Category of Loss	Description
Forensic and investigation costs	Forensic and investigative costs to preserve key evidence, identify the cause and extent of the threat actor's access, remove and remediate impacted systems, prepare relevant internal and external reports, support data restoration work and assist in notification processes.
Data restoration and system rebuild costs	Internal and external costs incurred to rebuild, remediate and test systems and applications, and to restore or re-create individual data assets and services.
System hardening and asset replacement costs	Expenses incurred to improve the overall security posture and controls which exist within the environment to a state beyond what existed before the cyber security event incurred.
Public relations and communication costs	Wide ranging costs to manage corporate, social and media messaging and communications resulting from cyber incidents.
Privacy and regulatory costs	Costs associated with managing and responding to relevant legal costs arising from the cyber security incident including claims and complaints by stakeholders and customers, privacy and data security obligations and privacy and data security notification processes.
Notification costs	Costs incurred to notify impacted individuals and advise them on the steps necessary to protect themselves from future harm. These costs include setting up and running a temporary call centre, customer/consumer notification, the provision of credit monitoring and in some cases identity protection services.
Loss of profits and business interruption	The amount of actual loss of business income sustained during the period of outage, or resulting from reputational harm arising from the adverse publication of an event. Common example include potential customers taking their business elsewhere, expenses ballooning in order to cover the cost of fixing weak security points, and to compensate customers and stakeholders.
Increased cost of working	Operational expenses incurred following a cyber event which are greater than the organisation's normal expenses and have been incurred to reduce or avoid loss and to maintain elements of functionality or to outsource key processes.
Support for impacted individuals and organisations	Costs incurred to reduce the risk of harm that may be suffered by vulnerable data subjects, and to mitigate the potential harms to organisations who sensitive third party data may be exposed by the cyber event.
Loss of value of impacted data assets	Losses arising due to publication and unauthorised disclosure or data assets which are compromised due to a cyber security event.
Civil liability	Major cyber events can result in a variety of legal claims brought against the organisation and its directors from contractual partners, data subjects, shareholders and business stakeholders.

Emerging Trends – Threat Landscape

Key Trends



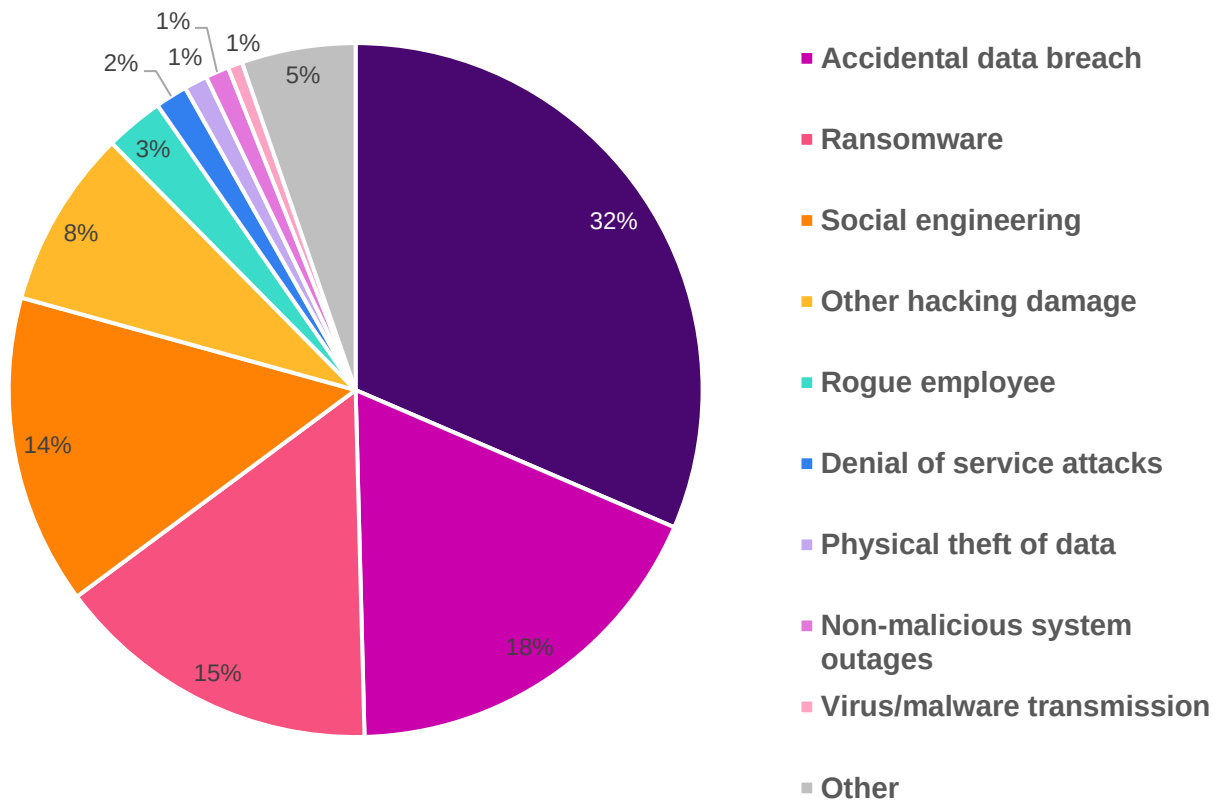
Consequences

- Greater **financial risks** from cyber events and increased exposure for **directors** and **senior leadership** where major incidents occur.
- Greater need to understand breach response support needs and key incident consequences. This includes **technology resilience, incident notification** steps, **communication strategies**, **harm assessments**, recovery and **stakeholder requirements**.
- Greater pressures being placed on information security budgeting and **resource allocation across cyber security priorities**.
- Renewed focus on **assurance processes** and extent to which objective **independent advice** is provided to senior management.
- Alignment of cyber security capabilities and processes with the **expectations of senior management** and independent directors.
- Significant pressures placed on **internal cyber security teams** (burn-out, retention challenges, skills uplift requirements).

Attack Chain Evolution

Re-Infections	Ransomware groups such as Scattered Spider and Akira are continuing to re-infect compromised organisations who fail to pay and are increasing their extortion demands for each subsequent attack.
MFA Bypass	Growing number of malicious cyber criminals deploying automated methods to trick victims into entering one-time passcodes, facilitating takeovers and undertaking communication interceptions.
Device / E-SIM Compromises	Malicious actors use the function provided by carriers for replacing or restoring a digital SIM card to transfer the victim's 'sim card'/phone number to their own device.
Trusted Insider Spoofing	Ransomware groups are increasingly pretending to be information technology (IT) help desk / and business support providers. To lend further credibility to their phishing attempts they often register domains similar to the domains of the legitimate organisation.
Adversarial AI/ML	Adversarial artificial intelligence and machine learning techniques seek to disrupt the operations of AI and ML systems. Malicious actors are also exploring the use of AI and ML technology to streamline and increase the success rates of traditional attacks.

WTW 2023 Cyber Claim Data



Expanding Social Engineering Methods

AI Whaling and AI Fraud attacks

An employee at a multinational construction engineering firm was manipulated into processing a series of transactions totalling over $200 million Hong Kong dollars – (about AUD $38.5 million).

The malicious actors used deepfake video technology to pose as company colleagues and as the company's chief financial officer.

The employee was tricked into attending a video call with what he thought were several other staff members, however these were deepfake recreations.

The employee also received a message that was purportedly from the company's UK-based chief financial officer. Initially, the worker suspected it was a phishing email, as it talked of the need for a secret transaction to be carried out. However, the worker put aside his doubts after the colleague video call because people in attendance had looked and sounded like colleagues he recognised.

Other Trends:

- Deep-fake technology to bypass KYC checks
- Voice phishing attack and audio spoofing
- Increasing use of synthetic media in cyber attacks

Misdirection of Cyber Incident Response Teams

Sophisticated ransomware groups have been found to leverage malicious cyber compromises and access to internal systems to help impersonate victim organisation team members and to frustrate incident response and recovery efforts.

Threat intelligence firms have identified several instances where ransomware groups attempted to pose as internal security teams and employees after the malicious compromise was identified.

In some cases, the threat actors joined incident remediation and response calls and teleconferences to identify the steps that security team were taking, and to get better insights into whether the organisation was likely to pay a cyber extortion demand.

The information obtained via these methods can also be used by the malicious actor to develop new intrusion techniques and to cause greater reputational harm to the victim organisation.

Other Trends:

- Threat actors tricking users into agreeing to unnecessary "technical support" services.
- Sometimes tied to link listing attacks –where threat actors sign up subscription services to flood email addresses.

Payments Coercion and Threats

Mandiant has reported an increase in incidents where threat actors attempted to impersonate the family member of victim organisation executives to convince them to pay a cyber extortion demand.

Malicious actors have used a variety of methods including caller ID spoofing, SIM swapping, and AI deepfake technology.

Some of the most harmful examples have been where a malicious actor has SIM swapped the phones of children of an executive, and then made calls to the executive from the phone numbers of their children.

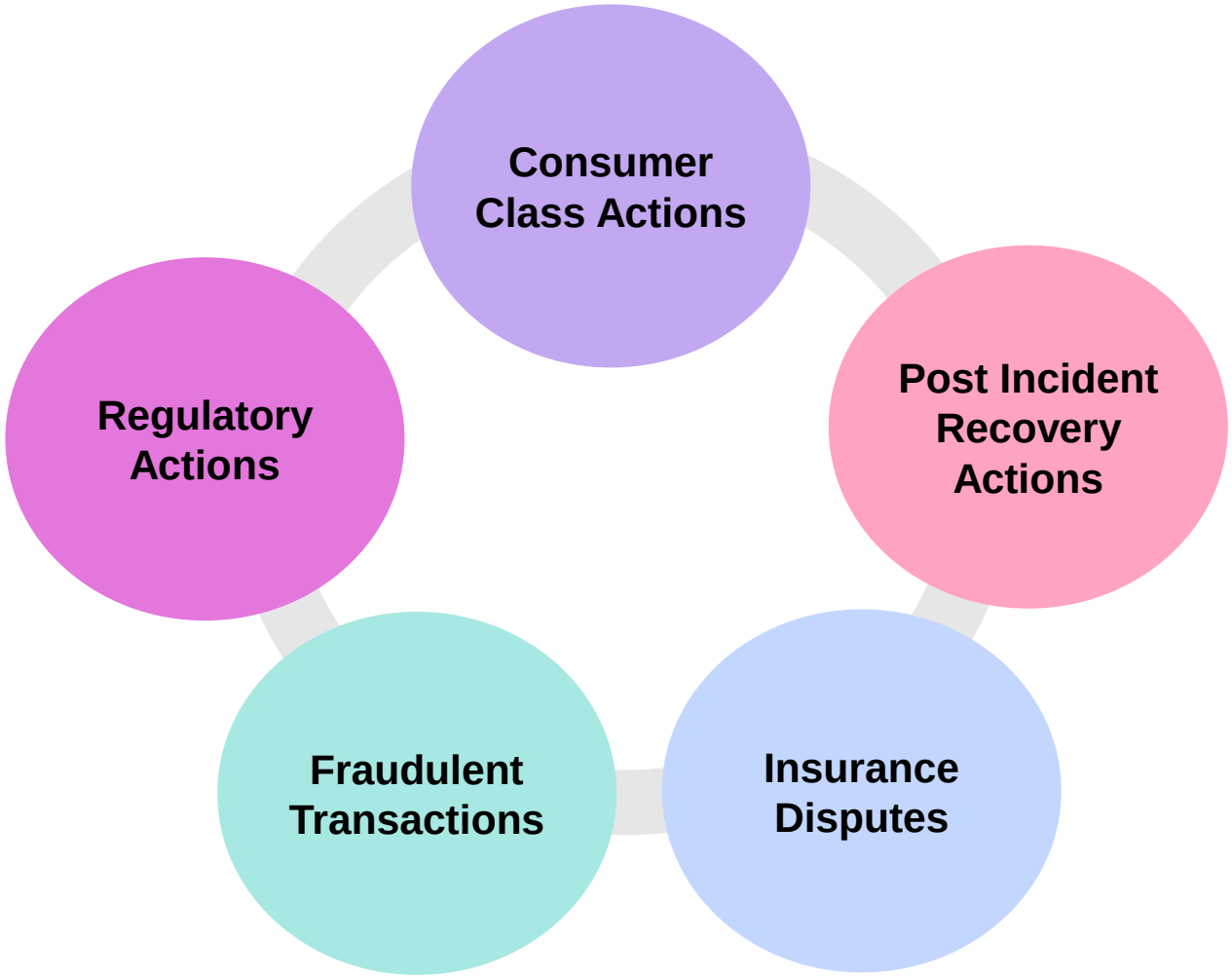
When the executive answers the call they will typically hear a stranger's voice, advising them to urgently make the payment or face consequences. These calls are typically made when the organisation stops responding to the threat actor or when ransom negotiations end.

Other Trends:

- Publication of ransomware negotiation logs.
- Personal extortion of data subject victims.
- Registering fake posts and comments on social media platforms purporting to be impacted data subjects.

Litigation and Legal Risk Cyber Consequences

Common Types of Litigated Disputes



> Cybersecurity, data protection and data privacy also top the list of litigation concerns in the year ahead amid the challenges posed by data management and AI.

Norton Rose Fulbright's 2024 Annual Litigation Trends Survey

> A federal panel on Friday centralized 49 lawsuits accusing UnitedHealth Group's Change Healthcare payment processing unit of failing to protect personal data from February's cyber attack in Minnesota.

Reuters – June 8 2024, Lawsuits over Change Healthcare data breach centralized in Minnesota

> Australia's privacy watchdog will take legal action against Medibank Private for failing to protect the medical details of 9.7 million Australians, which were accessed by Russian cybercriminals in 2022, with fines in the civil action potentially exceeding $21.5 trillion.

AFR – June 5 2024, Medibank faces maximum $21.5 trillion fine in new cyber hack case

Key Australian Class Actions – Optus and Medibank

	Optus 2022 Breach - Consumer Class Action	Medibank - Consumer Class Action 1 and 2		Medibank - Shareholder Class Action 1 and 2	
Status:	▪ On 27 May 2024, the full federal court upheld the primary decision that Optus' could not claim privilege over a Deloitte Report prepared following the incident. ▪ On 14 June 2024 Justice Beach flagged the possibility of merging these proceeding with the recent regulatory action brought by the Australian Communications and Media Authority.	▪ Consolidated on 1 August 2023 ▪ Maurice Blackburn Lawyers also lodged a representative complaint with the Australian Information Commissioner on November 18, 2022. ▪ On 19 June 2024 the Australian Information Commissioner filed civil penalty proceedings in the Federal Court.		▪ Consolidated on 6 September 2023. ▪ Group Costs Order accepted on 4 February 2024.	
Jurisdiction:	***Federal Court (Vic)***	***Federal Court (Vic)***		***Supreme Court (Vic)***	
Breach of contract	**Yes**	**Yes**	**Yes**	No	No
Negligence	**Yes**	No	**Yes**	No	No
Breach of confidence	No	**Yes**	No	No	No
Misleading or deceptive conduct	**Yes**	**Yes**	**Yes**	No	**Yes**
Breach of continuous disclosure obligations by not disclosing alleged deficiencies in privacy and cyber maturity	No	No	No	**Yes**	**Yes**
Loss or damage claimed	▪ Damages for non-economic damage caused by distress, frustration and/or disappointment not amounting to injury, and cost of time spent addressing consequences of the data breach. ▪ Orders to delete or de-identify all identifying document PI once they no longer have a valid purpose.			▪ Loss arising from drop in share price drop during the relevant period.	

Recovery Actions – Impacted Organisation Perspective

Organisations **retain significant losses** after a major cyber event:

Tabletop Example	
Lost Component	**Amount**
Incident Response Costs (Forensic, Legal, Privacy, Notification)	$1.3m
Extortion Demand / Extortion Expense	$0.5m
Data and System Recovery Loss	$1.9m
Business Interruption – Loss of Net Profit	$4.4m
Business Interruption – Extra Expenses/ correlating with NP	$0.3m
Assessment / Claim Preparation Costs	$0.2m
PCI-DSS	$0.2m
Regulatory and Third-Party Proceedings	$0.8m*
Mitigation Costs	$1.1m
Total:	**$10.7m***

** Still Developing*

Organisations also face a broad range of **consequential impacts**:

#	Scenario Name	Type of Scenario	# incidents
23	IT Configuration Errors enables fraudulent payments	**Privacy & Outage**	**0.01 / year** [17% of total incidents]
45	Phishing Attack causes PII breach moderate	**Privacy Breach**	**0.00 / year** [2% of total incidents]
81	Phishing-Ransomware leads Breach large	**Privacy & Outage**	**0.01 / year** [17% of total incidents]
38	Malware infection causes OT BI, Accident, Fatalities	**Privacy & Outage**	**0.01 / year** [17% of total incidents]
46	Ransomware leads to BI and Breach moderate	**Privacy & Outage**	**0.00 / year** [4% of total incidents]
52	Ransomware encrypts causes BI and Breach large	**Privacy & Outage**	**0.00 / year** [4% of total incidents]
65	Code Injection results in BI large	**Privacy & Outage**	**0.00 / year** [4% of total incidents]
77	Ransomware enables Breach and Loss of Data moderate	**Privacy & Outage**	**0.00 / year** [4% of total incidents]
7	Ransomware Drive-Wiper causes centralized backup server BI	**Privacy & Outage**	**0.00 / year** [2% of total incidents]
36	Nation State Attack-ransomware causes BI moderate	**Privacy & Outage**	**0.00 / year** [2% of total incidents]

Regulatory Actions

High level observations (this could be its own presentation):

1. Australia and Global Regulatory focus on cyber events and emerging obligations:

    - Australia – SOCI Reforms;
    - Australia – Proposed Cyber Security Act;
    - US – "Big Tech" – AMERICA Act;
    - US – SEC Rules on Cybersecurity – July 2023 & Oct 2023
    - EU – Cyber Security Regulation 2023/2841

2. Wider range of parties and subject matters driving regulatory actions:

    - Directors/Security Leaders – Solarwinds;
    - Data Brokers - X-Mode Social;
    - Mobile apps – GoodRx;
    - Online marketplaces – Drizly;
    - Breach response – Blackbaud / MoveIT; and
    - Public Statements and Disclosures – Solarwinds.

Does it turn on InfoSec Strategy?

Key complaints in *Australian information Commission v Medibank VID497/2024*:

- Implement proper change management controls for changes made to information security controls.
- Implement appropriate privileged access management controls.
- Implement appropriate monitoring for privileged accounts, including by monitoring to understand normal behaviour, configuring alerts, and monitoring alerts, for suspicious privileged account activities.
- Implement appropriate security monitoring processes.
- Review and triage of all security alerts generated by EDR Software.
- Configuring volumetric alerts to be generated for the large exfiltration activities.
- Implementing effective annual penetration testing and internal tests.
- Implement appropriate application controls for critical servers.
- Implement effective contractor assurance.

Insurance – Potential Coverage and Claim Issues

Proof of Loss - response challenges

Timeline pressures can result in poor documentation and a lack of clear evidence for why certain recovery steps were taken, and how incident response costs were incurred. This can often lead to concerns around gold plating (restoration beyond the pre-existing environment), whether vendors reasonable arose from the incident and what constituted wider environment uplift.

Insurance policy matching

There is significant variance between many of the insurance wordings used in the marketplace. Wordings can contain material differences in relation to policy exclusions, business interruption coverage, data restoration coverage, cyber extortion coverage and system failure coverage. Many brokers failure to understand this issue.

Threat actor behaviour

Specific attack chain steps that are performed by a malicious actor can significantly influence coverage e.g. whether malicious software is deployed, if data exfiltration occurs, whether backups are compromised, if supply chains are compromised and whether ingress is via legacy or unsupported technology assets.

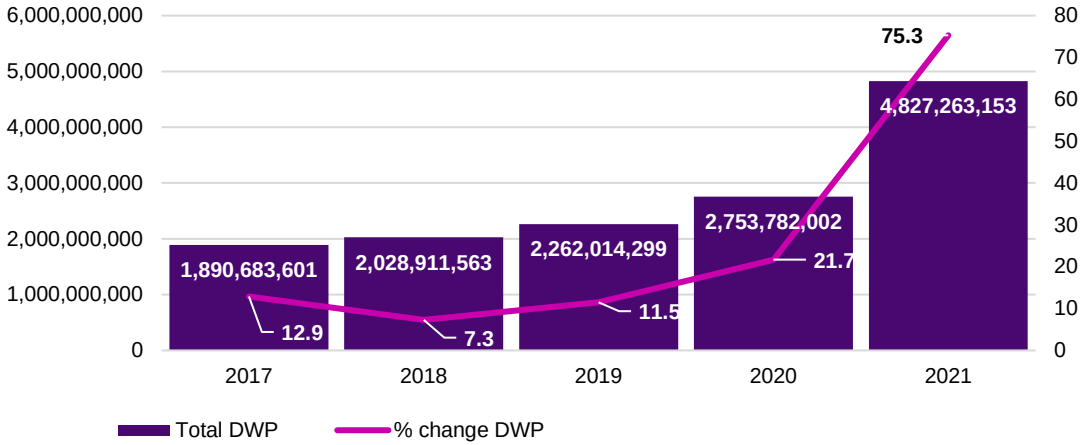
Whole of programme

Major cyber events increasingly have cross policy consequences (e.g. Cyber / PI / D&O / Crime / Property / M&A). No one policy can cover all the exposures, and the insurance programme must be collectively designed to maximise insurance coverage.

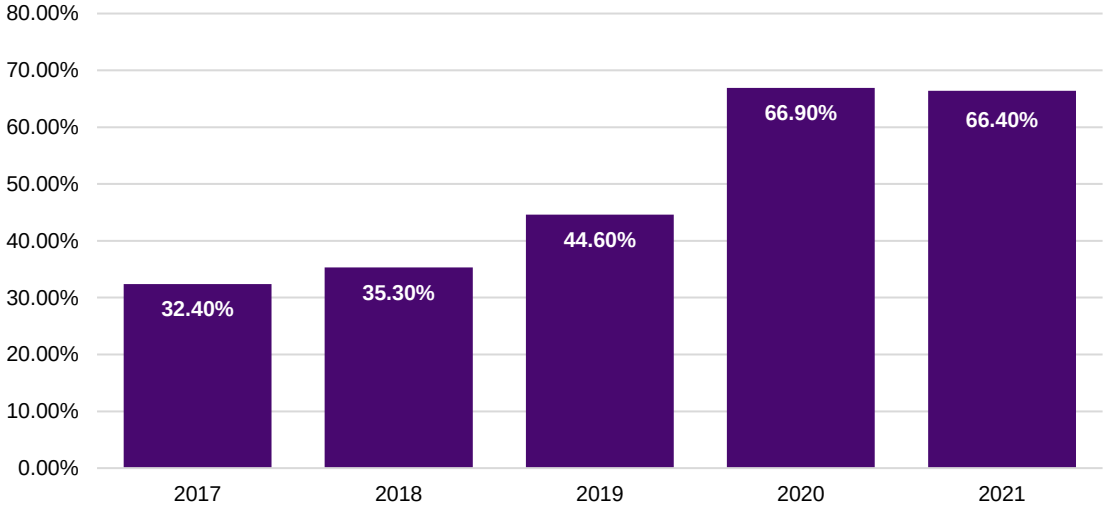
Submitted Questions

What profit margin do insurers expect? – NAIC Statistics

Cyber - market expansion



Cyber - Average loss ratio



Loss ratios: Top U.S. insurers

2021 Rank	2020 Rank	Group number	Group name	Direct written premium	Loss ratio w/DCC	Market share
1	1	626	Chubb Ltd Grp	473,073,308	76.9%	9.8%
2	8	158	Fairfax Fin Grp	436,447,801	51.9%	9.0%
3	2	968	AXA Ins Grp	421,013,729	86.5%	8.7%
4	11	3098	Tokio Marine Holdings Inc Grp	249,785,218	43.8%	5.2%
5	3	12	American Intl Grp	240,613,748	130.6%	5.0%
6	*	3548	Travelers Grp	232,276,831	72.7%	4.8%
7	5	4942	Beaziey Grp	200,877,555	38.7%	4.2%
8	7	218	CAN Ins Grp	181,382,785	87.5%	3.8%
9	*	1279	Arch Ins Grp.	171,944,995	9.2%	3.6%
10	6	3416	AXIS Capital Grp	159,059,212	105.2%	3.3%
11	13	212	Zurich Ins Grp	151,865,004	76.9%	3.1%
12	14	111	Liberty Mut Grp	138,216,723	95.2%	2.9%
13	12	3219	Sompo Grp	133,519,577	54.3%	2.8%
14	10	23	BCS Ins Grp	132,043,119	80.1%	2.7%
15	*	91	Hartford Fire & Cas Grp	123,163,166	16.3%	2.6%
16	*	361	Munich Re Grp	119,989,106	69.0%	2.5%
17	20	181	Swiss Re Grp	103,827,837	32.7%	2.2%
18	*	501	Alleghany Grp	88,554,222	20.5%	1.8%
19	*	98	WR Berkey Corp Grp	81,249,260	36.9%	1.7%
20	16	31	Berkshire Hathaway Grp	71,365,401	-0.5%	1.5%

*6 groups moved into the top 20 in 2020

For a professional IT services entity what are their most common uninsured areas?

Contract obligations	• IT service companies typically are required to agree to a broad range of warranties, indemnities, representations and assumption of liability clauses. It can be difficult to obtain full insurance coverage which matches all these contractual obligations. The best results will arise where an organisation seeks to maximise their whole of program insurance coverage (i.e. Cyber, Professional Indemnity, Crime, D&O, EPL and statutory liability).
Insurance Limit	• Many technology service organisations are under-insured. This is because they often do not account for their aggregative risk exposure, which arises because a failure in their technology stack or product offering has the potential to cause harm to all of their client collectively, creating the risk of multiple major claims arising from any major loss event.
Data Handling and Data Aggregations	• Broad range of obligations are taken on by technology service organisations in relation to how personal and service data is collected, stored, managed, processed and deleted. These obligations can create a range of harms including in relation to privacy, data sovereignty, information security, breach reporting, risk of harm assessments, post breach remediation, regulatory liability, civil liability and cyber security uplift requirements.
Emerging risks	• Technology companies often must account for emerging legal and regulatory obligations, due to the fast pace at which new laws are introduced to address changes in technology service offering and policy concerns. Current examples of this include the emerging regulations to address artificial intelligence, information security, privacy, digital identity and online safety.
Digital/Kinetic Perils	• It is often difficult to obtain insurance for data and electronic systems that may result in physical perils (fire, personal injury, property damage, physical business interruption).

What are the top five factors to consider when determining whether insurance is good value?

Understanding of Key Loss Exposure

- How well will an insurance policy respond to a critical cyber loss, or adverse technology event which the organisation would sustain?
- What is the realistic financial loss that a major cyber event would cause to the organisation?

Incident Response Framework

- Does the insurance policy provide access to market leader vendors, and a framework to augment the organisation existing cyber security mitigation capabilities?
- Is broad coverage given for data restoration, recovery, and remediation?

Ransomware

- Does the policy provide broad coverage to reimburse the organisation for the expenses it will incur to investigate, triage and mitigate a cyber extortion attack?
- What support will the insurer and its panel provide to help navigate ransomware dilemmas?

Regulatory and Third Party

- Broad coverage for the privacy and cyber security regulatory and third-party obligations which the organisation is likely to sustain. This cover will also need to be considered in conjunction with professional indemnity and directors & officers' insurance.

Supply Chain / Nation State / Cyber War

- Careful consideration should be given regarding the extent to which the policy will cover cyber security incidents arising from supply chain attacks, national state actions and cyber warfare incident.

Exclusion Language

- Many exclusion can have significant impact on the overall scope of coverage which is availability under the insurance policy. Language to consider includes Professional Services Exclusions, Infrastructure Exclusions, Neglected Systems Endorsements, and Reasonable Precaution Endorsements.

What are the warning signs of a potentially unreliable or inadequate policy?

Lack of policy matching	• Insurance terms should be tied to the specific needs and key exposures of the organisation. This will often require the support of an expert insurance broker who understand the organisation and available market coverages.
Pricing	• The industry is not “one size fit all” and each carriers have different policy terms and forms. Many cheaper policies and specifically designed with reduced coverages and limitations which can significant restrict how the policy would respond.
Significant policy restrictions	• Imposition of any co-insurances, or non-market standard exclusions. E.g. broad exclusions for professional of technology services, unpatched endpoint exclusions, failure to maintain exclusions.
Old language	• Many old policy forms will not be able to account for recent changes in the threat landscape (i.e., malicious actor behavior, cyber incident loss changes, regulatory developments and emerging stakeholder requirements). For older policy forms manuscript language is typically preferable.

Career Pathways: Cyber Insurance

There are no qualification requirements to work in the insurance industry, and more specifically the Cyber insurance industry.

Things we look for / regard favorably:

- Knowledge of cyber security controls and how technology stacks are managed
- Understanding of financial and professional services
- Knowledge of the broad threat landscape and challenges organisations face within the cyber and risk space
- Understanding of key regulations (Privacy Act, SOCI, CPS234, Corporations Act) and global laws

ANZIIF/NIBA qualifications are also favorable.

Common qualifications that individuals have when working in this space include:

- CISSP: Certified Information Systems Security Professional
- CISM: Certified Information Security Manager
- CRISC: Certified in Risk and Information Systems Control

Please note, these require a minimum number of years work experience within the industry.

WTW Cyber & Tech – Broader Perspective on Cyber Risk

Risk Advisory

1. Comprehensive Risk Assessments
2. Insurability Analysis
3. Governance enhancements & policy drafting
4. Cyber Incident Tabletop Exercises
5. Ransomware Preparedness
6. Board and Executive Risk Advisory
7. Supply Chain Risk Management
8. M&A Cyber Due Diligence

Risk Quantification

1. Cyber Risk Quantification
2. Cyber Benchmarking
3. Scenario Risk Modelling
4. Global & Local Cyber Claims data
5. Incident Response Costs
6. Regulatory and Civil Liability Risks
7. Business Continuity Impact

Education & Thought Leadership

WTW provided frequent thought leadership updates addressing key developments across the insurance, threat and technology landscape.

Insurance Placement

WTW specialises in difficult cyber and technology insurance risks. Our capabilities are unrivalled. We also design custom solutions for emerging and challenging risks.

> *"Thank you WTW team for the incredible work put into the drafting of the IRP and BCP over these past few months. The synergy between our organisations has been fantastic and your **excellent communication skills** paired with the **high quality of work** is greatly appreciated by our team."*

> *WTW played a crucial role in conducting **cyber crisis exercises/simulations**. As a trusted brand familiar to our board and executives, their insights greatly contributed to enhancing our processes… [and] were instrumental in **improving our response plans**.*

Questions