MARSH

Cyber Security: Business Vulnerabilities
SISA Forum

August 2020

Kelly Butler

Cyber Practice Leader - Pacific

MARSH & McLENNAN COMPANIES

Outline

- Cyber Risk Overview
- Current Threats and Trends
  - Threats Categories
  - Threat Examples
- Consequences of Cyber Security Threats
- Key Cyber Security Considerations
  - COVID19 Environment
- Consequences of Cyber Risk
- Cyber Insurance

Cyber Risk Overview

2020 Cyber Risk Landscape

Recap of 2019

Rising economic impact of cyb attacks: the global average cos breach in 2019 is USD3.9 mil

Cybercrime costs busin rillion

Changing risk perc r risk now ranks as a top risk; increasing owne agement and boards

Increased attention: changing legislatio evelance of mandatory notific

The hreat: vulnerabilities pos mployees

2020 Landscape

Targeted and more ambitious attacks: New and emerging attack groups, refinement of tools and tactics used, “living off the land”

New targets and access points: Supply chain attacks up 78% in 2019[1], Internet of Things devices highly susceptible and targeted. Critical infrastructures will be plagued by more attacks and production downtimes

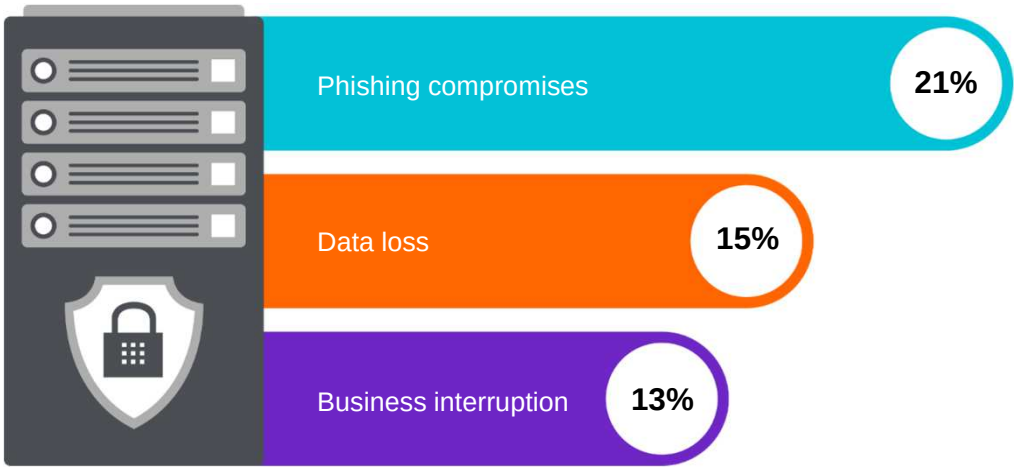
A global uptick in ransomware claims made them the most frequently reported claim of the year; 2019 statistics suggest an organisation will fall victim to ransomware every 14 seconds.

Less about security, but resiliency: cybersecurity spend in 2019 forecast to reach USD124billion, cyber-attacks cost the world economy USD600billion each year. Focus on resiliency, the ability to prepare for, respond to and recover from a cyber attack.

Cyber Risk Overview

Most common types of cyber incidents experienced in 2019-20

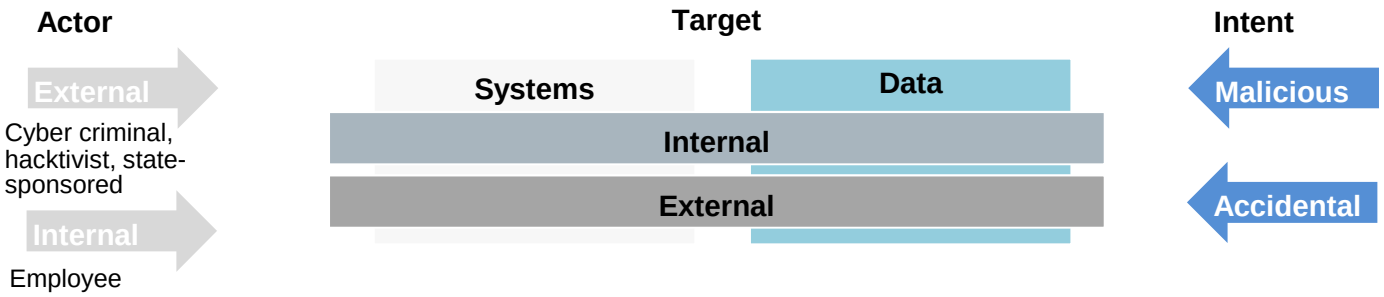
Most common incidents Australian Small to Medium business faced in the past 12 months:



Cyber Security Threats

Cyber Is A Complex Set Of Risks That Can Lead To Multiple Impacts

But it can be broken down into components



Immediate impacts

Systems not available or malfunctioning

Data stolen, deleted, corrupted or changed

Potential business impacts

- Response costs (notification, investigation, clean-up)
- Loss of revenue
- Legal liability
- Reputational damage
- Loss of intellectual property / critical data
- Fines

Current Threats and Trends
Threat Actors

Threat Matrix	Organised Crime	Script-Kiddies, Lone Wolves, Other Malcontents	APT's	Insider Threats	Hacktivist
Motivation	Money	Fun, Curiosity	Strategic	Malicious Intent, eroor, Negligence	Politics, Ethics
Choice of targets	Individual, by chance or directly aimed	By chance, political reasons	Individual, collateral	Employers, Unintentional	Ideological and political targets
Organisation	Strongly pronounced	Partially	Perfect	Individual/ partially	Structured
Competence	High	Low-High	Very-High	Low-High (external help)	Middle-High

Current Threats and Trends
Example of Current Threats

907k
Total Spam Messages related to COVID-19

737
Detected malware related to COVID-19

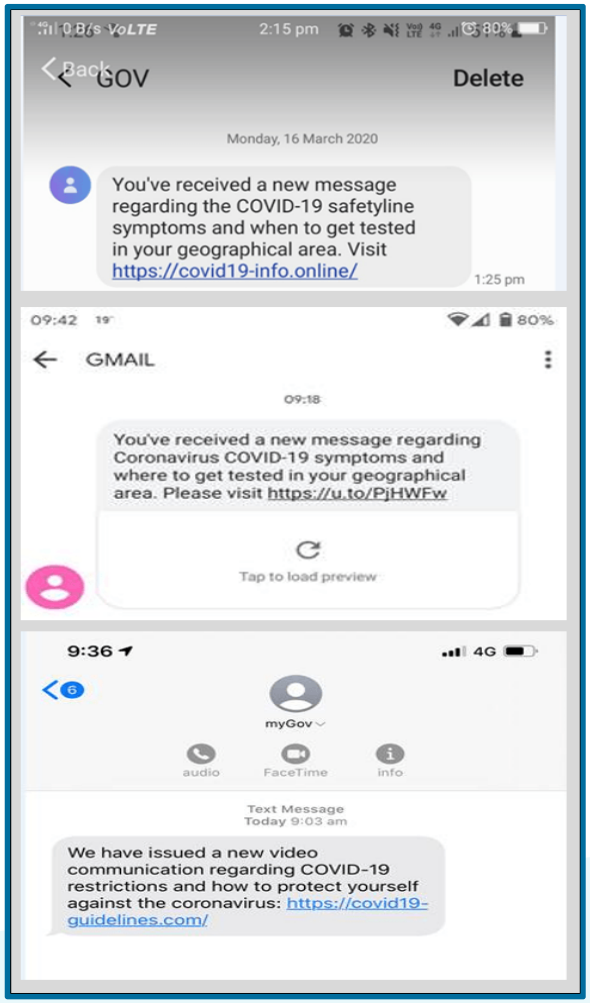
48k
Hits on malicious URL

220x
Increase in spam from Feb to Mar 2020

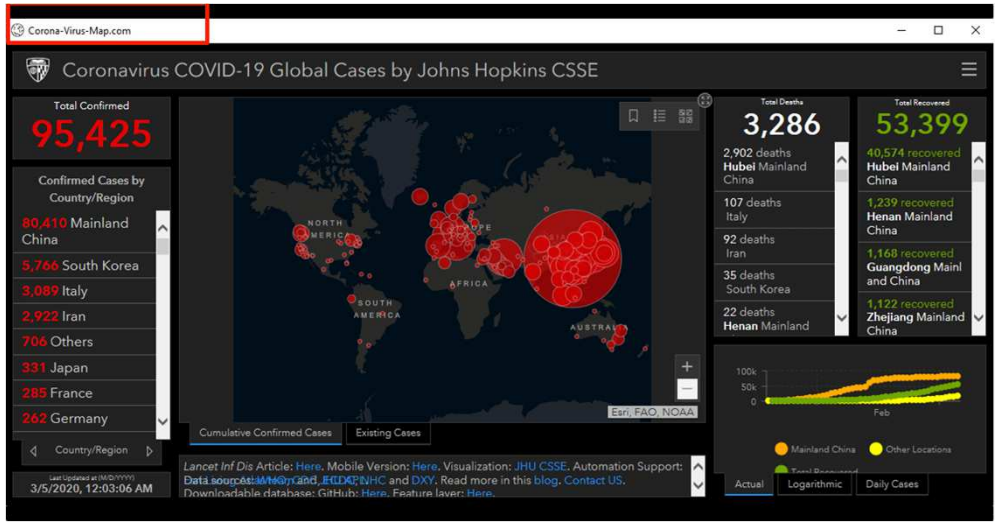
260%
Increase in malicious URL hits from Feb to Mar 2020

Current Threats and Trends
Examples of Current Threats

- 19th March, SMS phishing campaign recommences using a different number and sender name (GMAIL
- 16th March, Australians begin receiving text messages from malicious actors impersonating the government.
- 20th March, Malicious Actors utilise the alpha tag ‘myGOV’

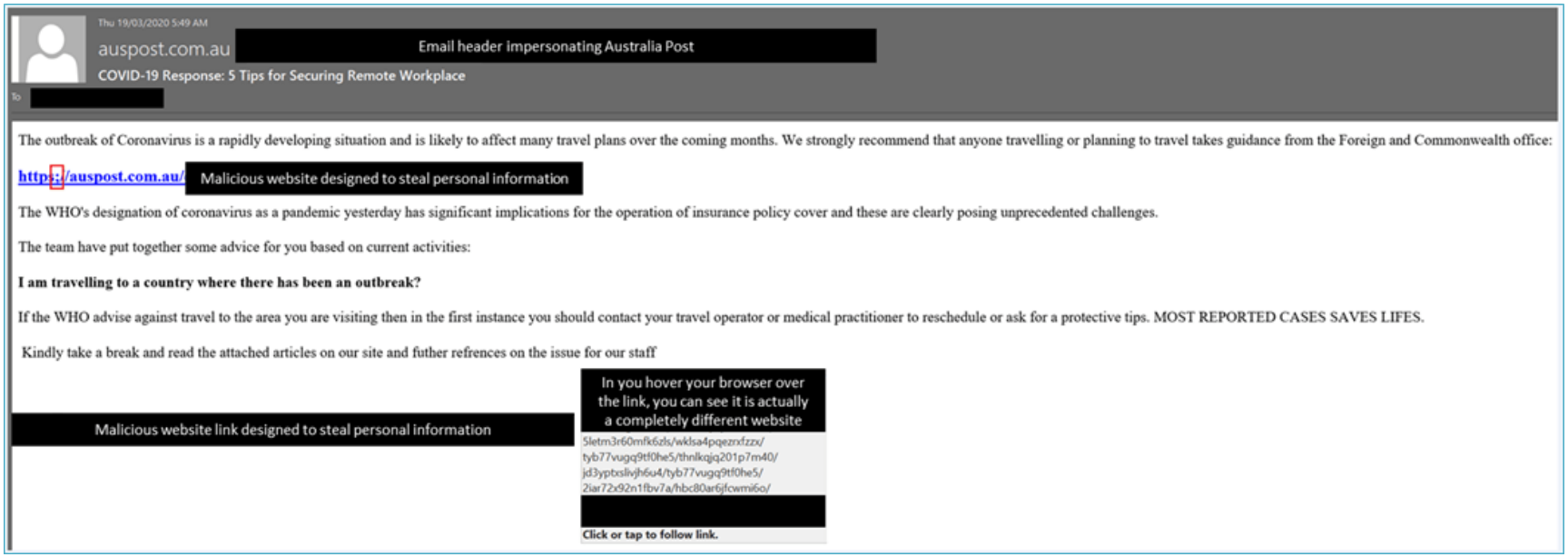


Current Threats and Trends
Example of Current Threats



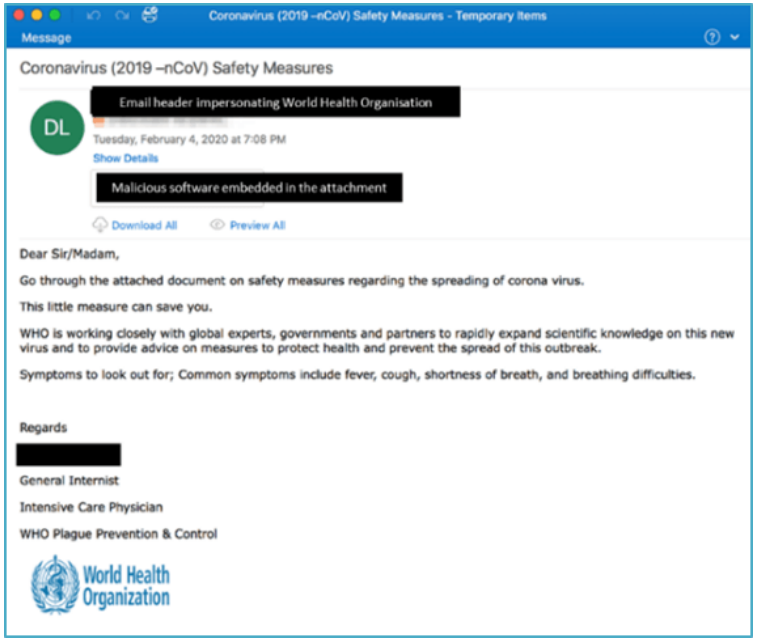
- Links often lead to fraudulent sites impersonating reliable sources.
- This is an example of a fake website impersonating the Johns Hopkins Coronavirus resource Centre.
- This is a process called **Pharming**

Current Threats and Trends
Example of Current Threats



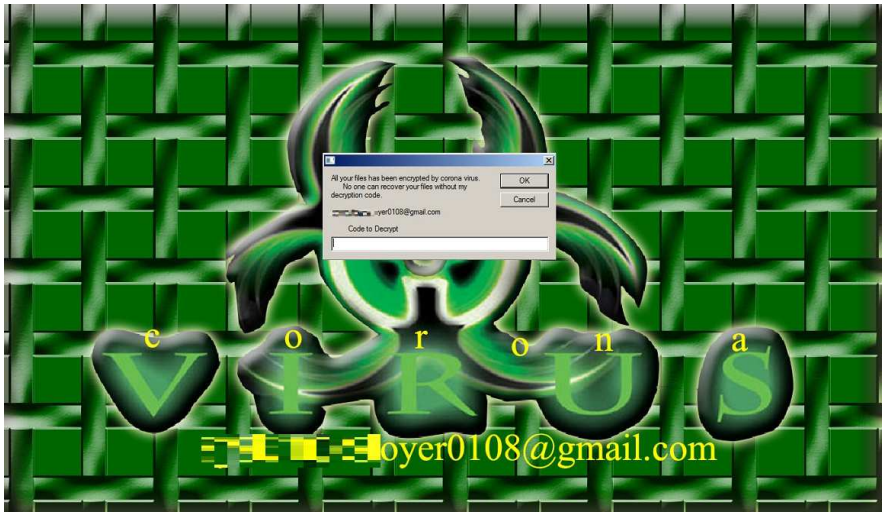
- 19th March, the ACSC received a report from Australia Post about a COVID-19 phishing email that was impersonating their organisation.

Current Threats and Trends
Example of Current Threats



- The ACSC has also received reports of COVID-19 phishing emails that have malicious Word documents or other attachments containing embedded computer viruses.
- When opened, the attached file contains malicious software that automatically downloads onto the recipient's device,

Current Threats and Trends
Example of Current Threats



- These attachments contain malware.
- An internet security provider recently analysed a coronavirus-themed malware that overrides a systems' master boot record (MBR), making it unbootable. Forcing victims to pay to access data.

Cyber Security Threats
Consequences – Data Breach

- Once attackers have gained access to sensitive information, these can be used for nefarious purposes
- Sensitive personal and payment card data can be monetised by selling to other criminal or through identity theft
- Other potential consequences include theft of trade secrets

Cyber Security Threats
Consequences – Misappropriation of funds

- Once a system is breached, attackers are able to monitor internal communications
- Attackers could then use the information to impersonate executives or vendors to scam funds
- Spoofing, Business Email Compromise, and payment gateway hijacking are potential outcomes


New Reply Reply to All Forward Display More

Confidential: Sensitive Transaction

John Smith to Jane Doe 31/03/2015 15:20

Show Details

Jane, *[a member of the finance team / FD / CFO]*

Your assistance is required in support of a sensitive transaction, which takes priority over all other tasks.

I shall arrange for XYZ LLP *[a professional advisory firm]* to make contact to discuss the finer details.

To avoid the risk of leakage to the press, or unwarranted interest from our regulator, under no circumstances must this be discussed outside of XYZ LLP and I.

Many thanks in advance for your support,

John *[typically the Managing Director / CEO]*

Key Cyber Security Considerations

Below an overview of key cybersecurity aspects to be considered by your IT/IS department

Awareness and training

Key concepts related to the cyber-risks in a teleworking environment the users are exposed to.

Incident response

Capabilities deployed and tested for responding in case a cyber incident is identified.

Security event monitoring

Critical characteristics related to the timely detection of cyber security incidents.

Vulnerability Management

Critical topics related to the vulnerability life cycle in the organization.

Security Architecture

Perimeter security components and remote connections.

Mobile Devices

Security configuration of mobile devices.

Workstations

Cyber security considerations for the configuration and usage of workstations.

Access Management

Aspects related to the processes that ensure that only the authorized users have the rights to access the systems in the organization.

Key Cyber Security Considerations

Cyber security good practices to be considered for your employees

Increase awareness for potential COVID-19 email/phishing scams.

Prevent usage of personal email/file sharing services.

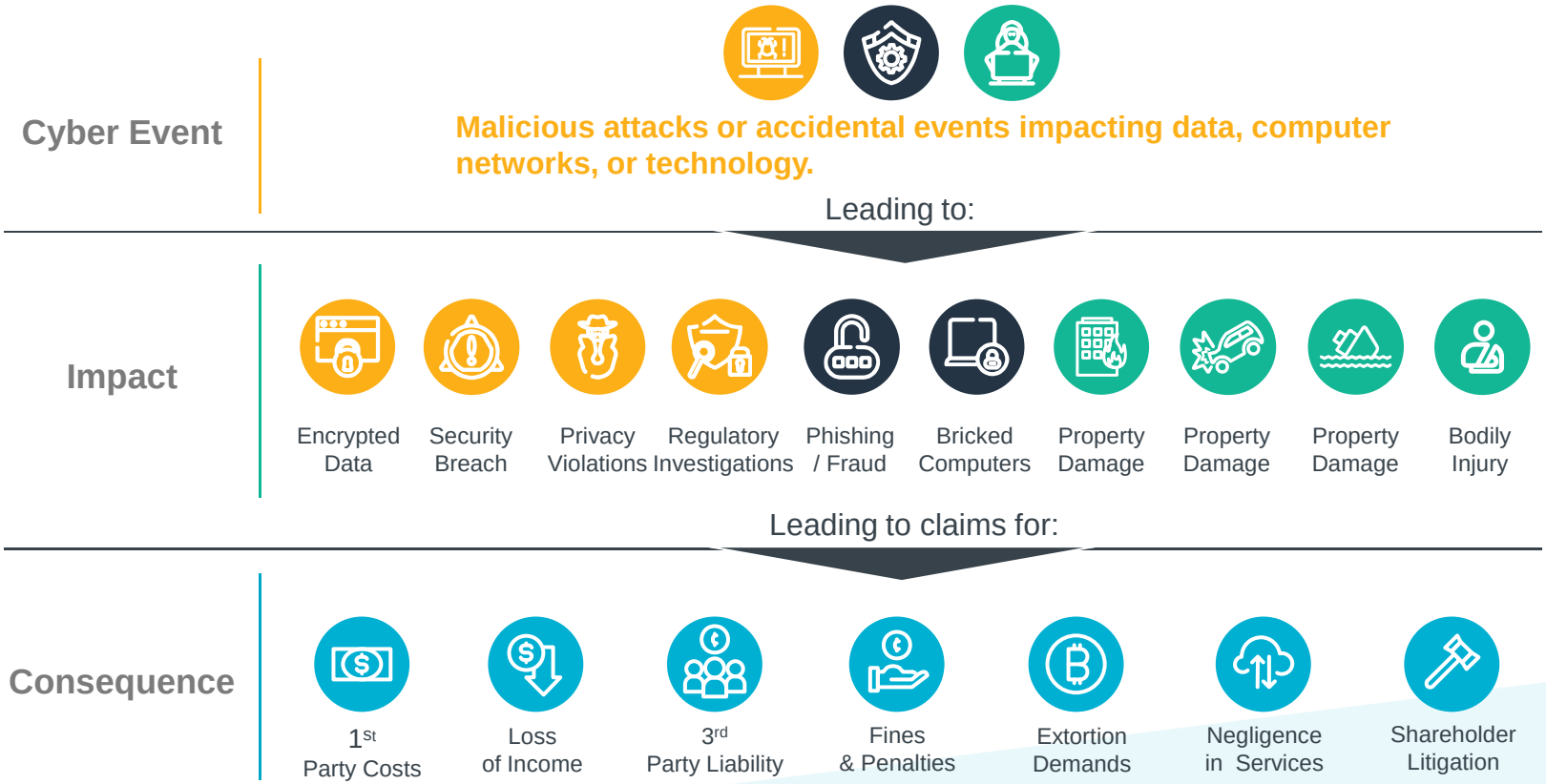
Prevent copying work files to personal devices.

Mute or shut down any digital assistant (e.g. Alexa, Google Assistant, etc.), since they are constantly recording nearby conversations.

Don’t let family members or friends use your company-provided equipment (e.g. laptop, phone, etc.).

When printing at home, secure paper files in a safe place after you finish working.

Consequences of Cyber Risk



Cyber Insurance: Core First Party Coverages

Direct loss and out of pocket expense incurred by an insured

COVERAGE	DESCRIPTION	COVERED COSTS
Business Interruption / Extra Expense	Interruption or suspension of computer systems due to a network security breach. Coverage may be limited to security attacks or broadened to include general system failure.	▪ Loss of Income. ▪ Costs in excess of normal operating expenses required to restore systems. ▪ Forensic expenses to value a loss. ▪ May include contingent business interruption as well.
Data Asset Protection	Costs to restore, recreate, or recollect your data and other intangible assets that are corrupted or destroyed by a cyber attack.	▪ Restoration of corrupted data. ▪ Vendor costs to recreate lost data.
Event Management/Breach Response	Costs resulting from a network security or privacy breach.	▪ Forensics. ▪ Notification. ▪ Credit Monitoring. ▪ Call Center. ▪ Public Relations.
Cyber Extortion	Threat to compromise network or data if ransom not paid.	▪ Forensics and related investigation costs. ▪ Costs to negotiate and pay any ransoms demanded.
Cyber Crime / Social Engineering	Funds transferred inerrpr	

Cyber Insurance: Core Third Party Coverages

Defence and liability incurred for damage to others, caused by an insured

COVERAGE	DESCRIPTION	COVERED COSTS
Privacy Liability	Failure to prevent unauthorised access, disclosure or collection, or failure of others to whom you have entrusted such information, for not properly notifying of a privacy breach.	▪ Liability and defense costs. ▪ Commercial litigation – e.g., bank suits. ▪ Consumer litigation – e.g., class-actions. ▪ Third-party costs for notification and investigation. ▪ PCI fines and penalties.
Network Security Liability	Failure of system security to prevent or mitigate a computer attack. Failure of system security includes failure of written policies and procedures addressing technology use.	▪ Liability and defense costs. ▪ See above.
Privacy Regulatory Defense Costs	Privacy breach and related fines or penalties assessed by Regulators.	▪ Liability and defense costs. ▪ Regulatory investigations. ▪ Insurable fines and penalties. ▪ Prep costs to testify before regulators.
Media Liability	Defense and liability for online libel, slander, disparagement, misappropriation of name or likeness, plagiarism, copyright infringement, negligence in content to those that relied on content.	▪ Liability and defense costs. ▪ Commercial litigation – e.g., bank suits. ▪ Consumer litigation – e.g., class-actions.

Key Cyber Security Considerations

Financial Impacts and how can Cyber Insurance assist

Potential business impacts	Typical Coverages
Responses Cost (investigation, (notification, clean-up)	Breach/event response
Loss of revenue, additional costs of working	Network business interruption
Legal Liabilities	Ransomware event costs
Reputation Damage	Data recovery and restoration
Ransom demands	Privacy Liability
Costs to restore or recreate data	Reputational Harm
Costs to restore or rebuild systems	Contingent business interruption
	Privacy regulatory defense
	Pre-breach loss presentation and mitigation

Cyber Insurance Submission Recommendations
Marsh Recommended Best Practice for Cyber Risk Management

Enterprise-level Governance: Management ownership by all key organisational stakeholders.

Risk Identification: Assessment of cyber risk vulnerabilities, clarity on where the key exposures lie. Have an active understanding of the cyber threat landscape and its impact on your business.

Holistic Approach to Build Cyber Resilience: Manage cyber risk like other strategic risks, with a comprehensive approach that employs planning, mitigation, risk transfer and testing of response scenarios. Cyber insurance has an essential role to play in this solution.

Q&A


MARSH


MARSH & McLENNAN
COMPANIES