RISK NZ

WELCOME TO
RISKNZ’s LUNCHTIME SEMINAR SERIES 2019

RiskNZ would like to thank the support of our Sponsors and Hosts

PREMIER SPONSORS

JLT

SAI GLOBAL

LUNCHTIME SEMINAR SPONSORS:

Cybercraft

Safety Associates

LUNCHTIME SEMINAR SUPPORTERS - HOST VENUES

KPMG

NAVIGATUS CONSULTING

Christchurch City Council

POWERCO

Cybercraft

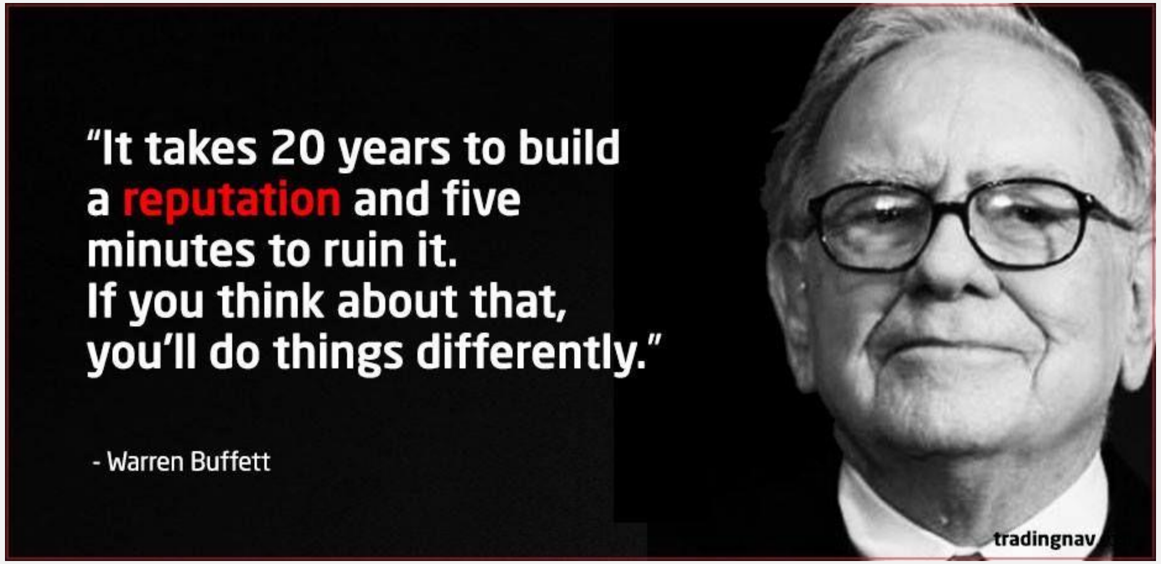
Building an active cyber responsibly culture for better business results

RISK NZ

Cyber risk lunchtime workshop

Why do we need a Cyber Responsibility Programme?

#1 Reputation



"It takes 20 years to build a reputation and five minutes to ruin it. If you think about that, you'll do things differently."

- Warren Buffett

#2 Continuous Change

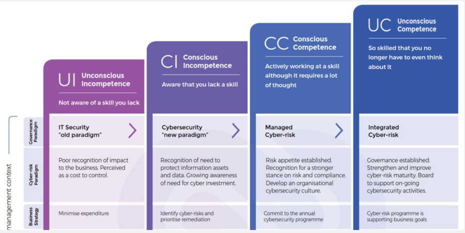
Everything is changing constantly, and every aspect of cyber risk management is interrelated.

So, when one thing changes, it impacts everything else. How can you possibly benchmark cyber risk management at any point in time? You can't.

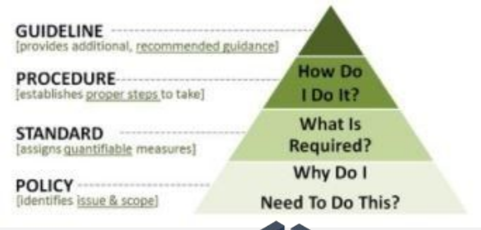
This means we must accept this realisation and strive for continuous risk management measurement.

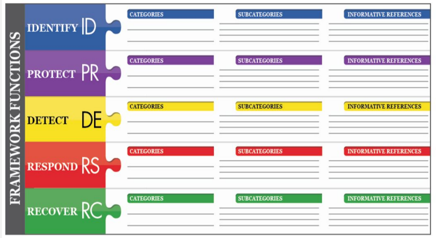
Jon Oltsik, CSO (2018)

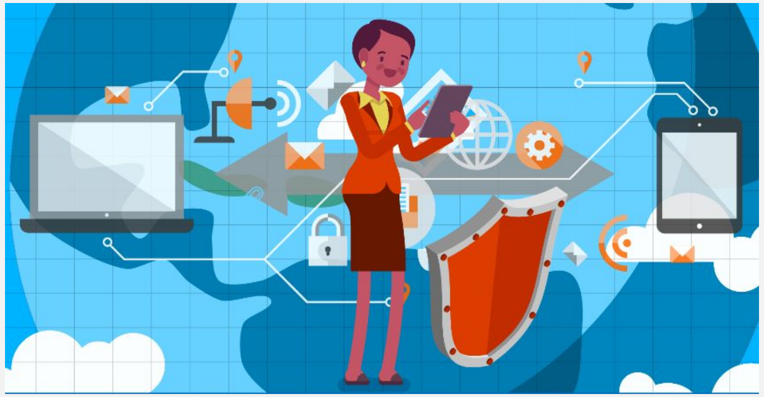
Why do we need a Cyber Responsibility Programme?

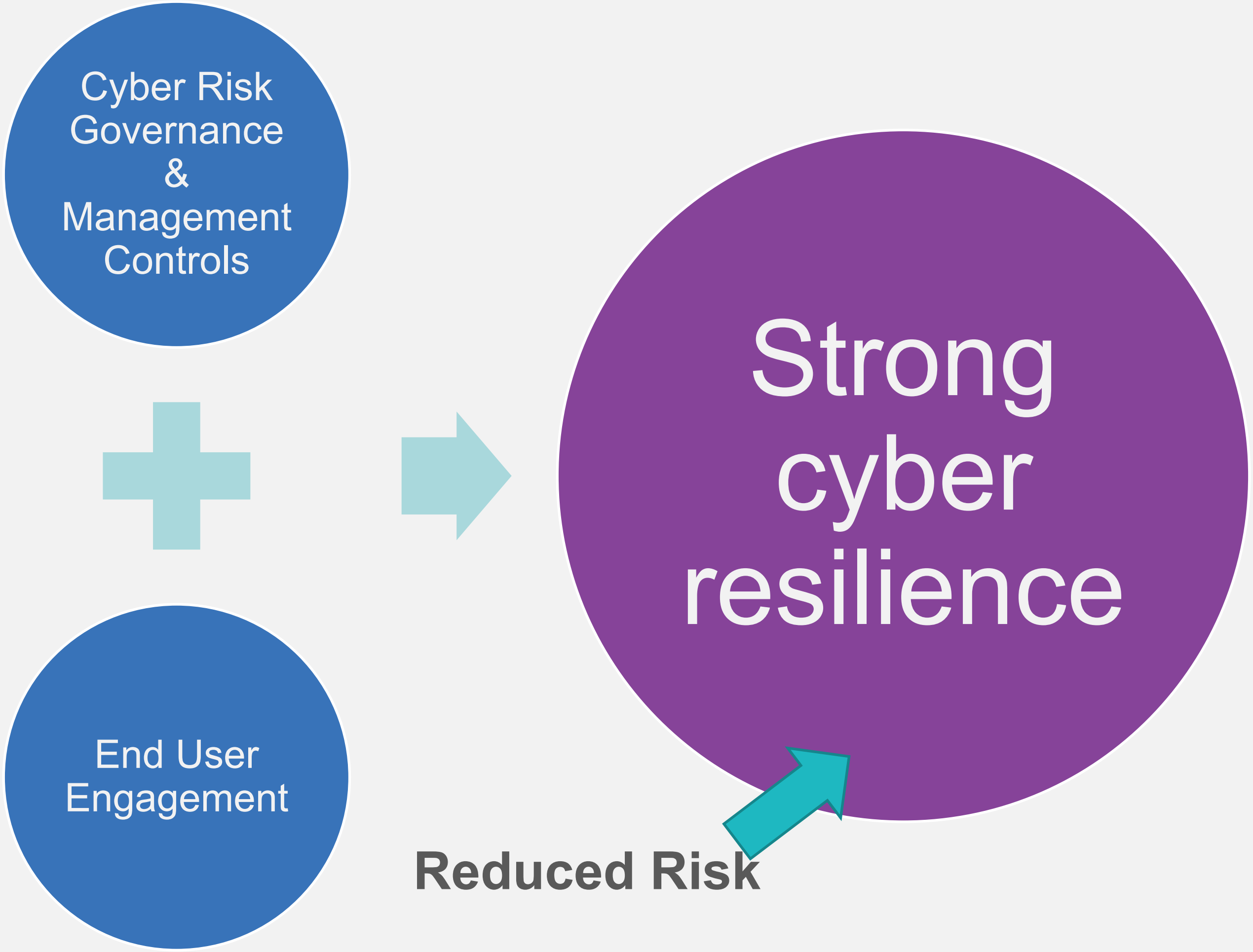


management context	UI Unconscious Incompetence Not aware of a skill you lack	CI Conscious Incompetence Aware that you lack a skill	CC Conscious Competence Actively working at a skill although it requires a lot of thought	UC Unconscious Competence So skilled that you no longer have to even think about it
Governance Paradigm	IT Security "old paradigm"	Cybersecurity "new paradigm"	Managed Cyber-risk	Integrated Cyber-risk
Cyber-risk Paradigm	Poor recognition of impact to the business. Perceived as a cost to control.	Recognition of need to protect information assets and data. Growing awareness of need for cyber investment.	Risk appetite established. Recognition for a stronger stance on risk and compliance. Develop an organisational cybersecurity culture.	Governance established. Strengthen and improve cyber-risk maturity. Board to support on-going cybersecurity activities.
Business Strategy	Minimise expenditure	Identify cyber-risks and prioritise remediation	Commit to the annual cybersecurity programme	Cyber-risk programme is supporting business goals


GUIDELINE
[provides additional, recommended guidance]
PROCEDURE
[establishes proper steps to take]
STANDARD
[assigns quantifiable measures]
POLICY
[identifies issue & scope]
How Do I Do It?
What Is Required?
Why Do I Need To Do This?







Cyber Risk Governance & Management Controls

End User Engagement

Strong cyber resilience

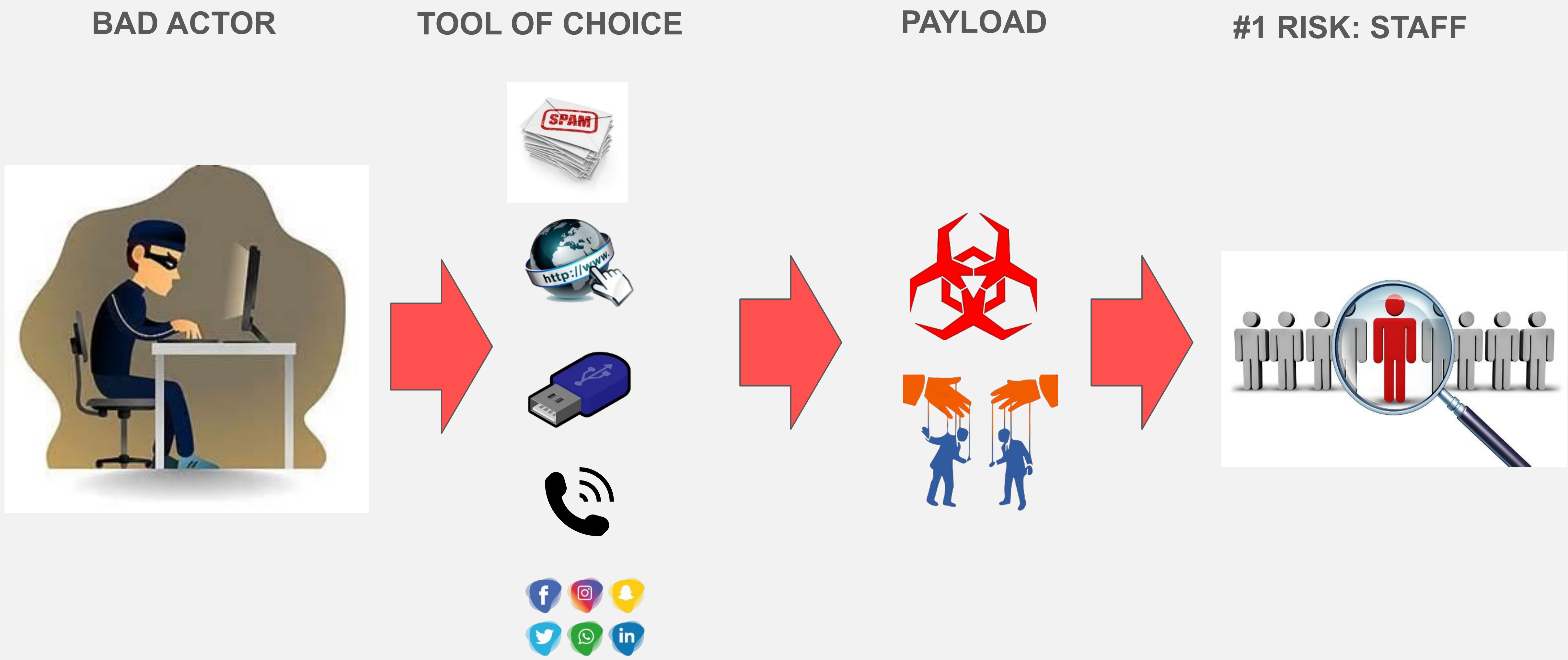
Reduced Risk

Why do we need a Cyber Responsibility Programme?

People are far easier to hack, and are still the biggest risk

Essential to develop cyber resilience within

The Practical Dangers of Cyberspace



BAD ACTOR

TOOL OF CHOICE

PAYLOAD

#1 RISK: STAFF

Resultant Loss and Costs

#1 RISK: YOU

DATA LOSS

BAD ACTOR

PASSWORD
**********_
Name
Second name
Initials
Address
Tel
Email
Protect Patient Information
bitcoin
IT Support

DIRECT COSTS

Our Goal

Build an active cyber responsibility culture for better business results

- Establish a consistent vigilance across the organisation to improve cyber resilience
- Visibility of importance of cyber responsibility and how it relates to the business objectives

By

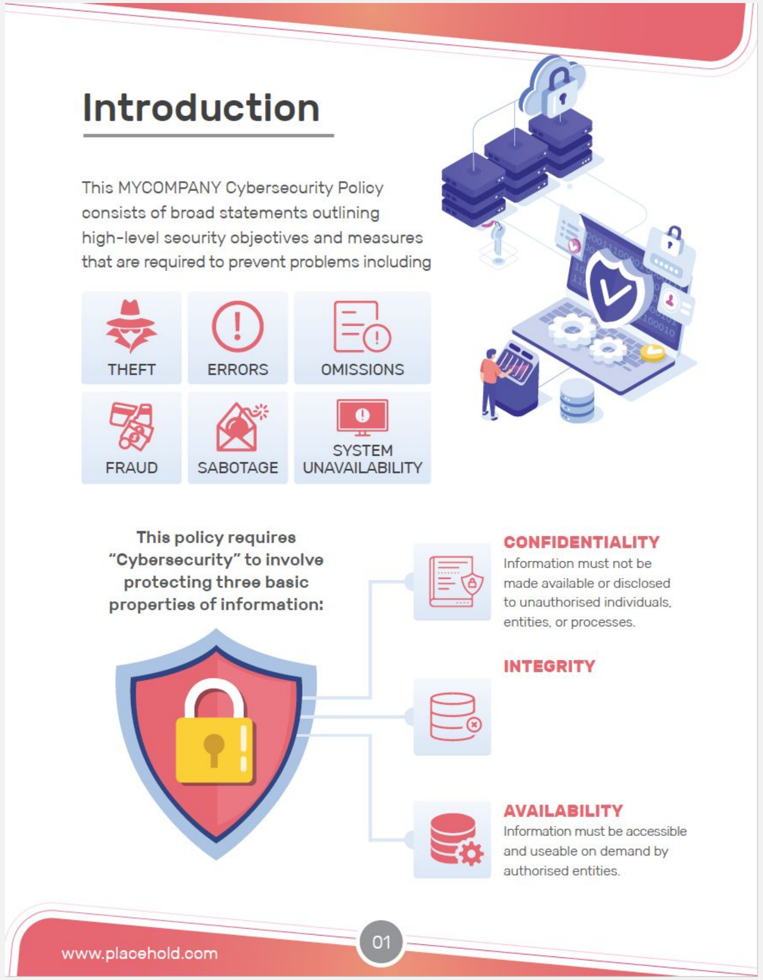
- Encouraging individual responsibility
- Become user-centric. Make policies user friendly – ebook or infographic
- Demonstrating commitment (that means investment) through workshops and training
- **Making cyber responsibility fun and interesting - gamification**

User friendly cybersecurity policy

CYBER SECURITY POLICY

PLACEHOLDER

www.placehold.com



Introduction

This MYCOMPANY Cybersecurity Policy consists of broad statements outlining high-level security objectives and measures that are required to prevent problems including

THEFT	ERRORS	OMISSIONS
FRAUD	SABOTAGE	SYSTEM UNAVAILABILITY

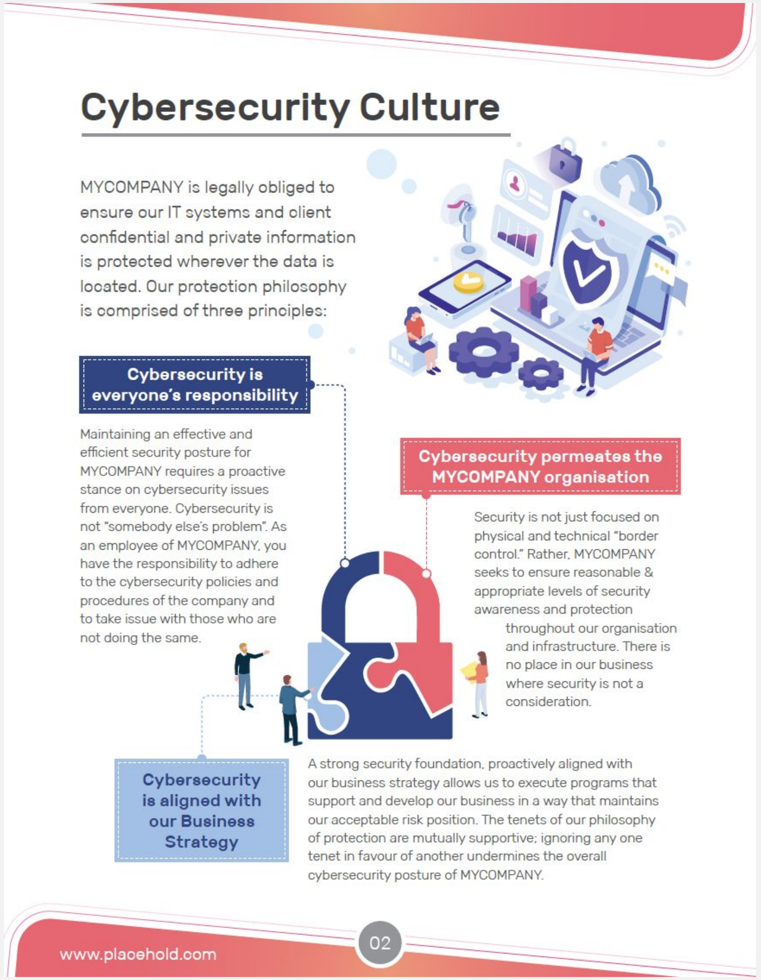
This policy requires "Cybersecurity" to involve protecting three basic properties of information:

CONFIDENTIALITY
Information must not be made available or disclosed to unauthorised individuals, entities, or processes.

INTEGRITY

AVAILABILITY
Information must be accessible and useable on demand by authorised entities.

www.placehold.com 01



Cybersecurity Culture

MYCOMPANY is legally obliged to ensure our IT systems and client confidential and private information is protected wherever the data is located. Our protection philosophy is comprised of three principles:

Cybersecurity is everyone's responsibility

Maintaining an effective and efficient security posture for MYCOMPANY requires a proactive stance on cybersecurity issues from everyone. Cybersecurity is not "somebody else's problem". As an employee of MYCOMPANY, you have the responsibility to adhere to the cybersecurity policies and procedures of the company and to take issue with those who are not doing the same.

Cybersecurity permeates the MYCOMPANY organisation

Security is not just focused on physical and technical "border control." Rather, MYCOMPANY seeks to ensure reasonable & appropriate levels of security awareness and protection throughout our organisation and infrastructure. There is no place in our business where security is not a consideration.

Cybersecurity is aligned with our Business Strategy

A strong security foundation, proactively aligned with our business strategy allows us to execute programs that support and develop our business in a way that maintains our acceptable risk position. The tenets of our philosophy of protection are mutually supportive; ignoring any one tenet in favour of another undermines the overall cybersecurity posture of MYCOMPANY.

www.placehold.com 02

Annual Cyber Responsibility Programme

Activities	Q1	Q2	Q3	Q4
Cybersecurity Policies	Cybersecurity Policy	Acceptable Use Policy	BYOD Policy	
Phishing Assurance	Baseline	Monthly Assurance	Monthly Assurance	Monthly Assurance
What to do in a…	Cybersecurity Emergency			Privacy Breach
Communications	Seasonal messages & hot topics	Identity and privacy	Cyber awareness for family & home	Board affirmation, achievements
Cyber Week		Internal seminar, posters, games etc		CERT National Cyber Week
Cyber Responsibility Workshops		Digital Citizenship	Family & Home	Privacy & data confidentiality
Procedures	Payments policy and procedures	Staff onboarding & exit procedures	Information Classification	

Following through to get engagement

- **Cadence:** Organisations can only absorb so much change at once
- **Gamification:** Create challenges & competition
- **Measure:** Monitor and improve the effectiveness of cyber training
- **Reward:** Recognise positive cyber responsibility behaviours
- **Incentivise:** Bring family and children into the picture

Better Cyber Risk Governance for Business

A pragmatic workshop to drive cyber risk engagement

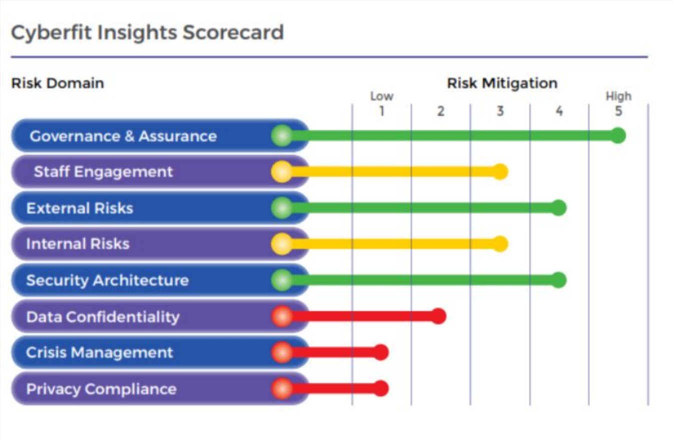
- Understand the importance of differentiating cyber risk and cybersecurity
- Determine cyber risk appetite in the context of your business
- Improve your cyber risk governance practices
- Apply the four dimensions of cyber risk operational governance
- Learn how to launch and drive a cyber responsibility culture in your business

How Cybercraft can help you

Cybercraft

Our role is to support directors and executives improve organisational cyber resilience through development of robust cyber risk governance and management practices.

Cyberfit Insights Assessment provides you with key insights into cyber risks within your organisation, determining risk and impact across eight primary cyber risk domains.

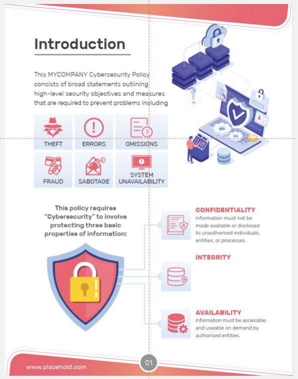


Cybersecurity Policies enables business management to define the cybersecurity directives for risk management that ensures consistency and compliance with the company's mission, values and strategic goals.

CYBER SECURITY POLICY

PLACEHOLDER

www.placehold.com



Introduction

This MYCOMPANY Cybersecurity Policy consists of broad statements outlining high-level security objectives and measures that are required to prevent problems including

THEFT
ERRORS
OMISSIONS
FRAUD
SABOTAGE
SYSTEM UNAVAILABILITY

This policy requires "Cybersecurity" to involve protecting three basic properties of information:

CONFIDENTIALITY
Information must not be made available or disclosed to unauthorised individuals, entities, or processes.

INTEGRITY

AVAILABILITY
Information must be accessible and useable on demand by authorised entities.

www.placehold.com 01

Chief Information Security Officer undertakes advisory or delivery roles for cyber risk management within your organisation. Develops and leads cyber risk strategy & management, and cybersecurity and awareness programmes.

AUCKLAND
Jeff Herbert
Director Cybersecurity & Blockchain

CHRISTCHURCH
Richard Williams
Director Cybersecurity & Privacy

Start a conversation with us

Hi, my name is Farah. My role is to facilitate the conversation around cyber risk management, how we may be able to help, and what engaging with Cybercraft might look like. Give me a call or send an email, I'd love to chat and help.

Farah Herbert

- Business Development Manager
- farah.herbert@cybercraft.net
- Mobile: +64 27 2200 111

RiskNZ would like to thank the support of our Sponsors and Hosts

PREMIER SPONSORS

JLT

SAI GLOBAL

LUNCHTIME SEMINAR SPONSORS:

Cybercraft

Safety Associates

LUNCHTIME SEMINAR SUPPORTERS - HOST VENUES

KPMG

NAVIGATUS CONSULTING

Christchurch City Council

POWERCO

RISK NZ

THANK YOU FOR ATTENDING OUR LUNCHTIME SEMINAR SERIES