KPMG

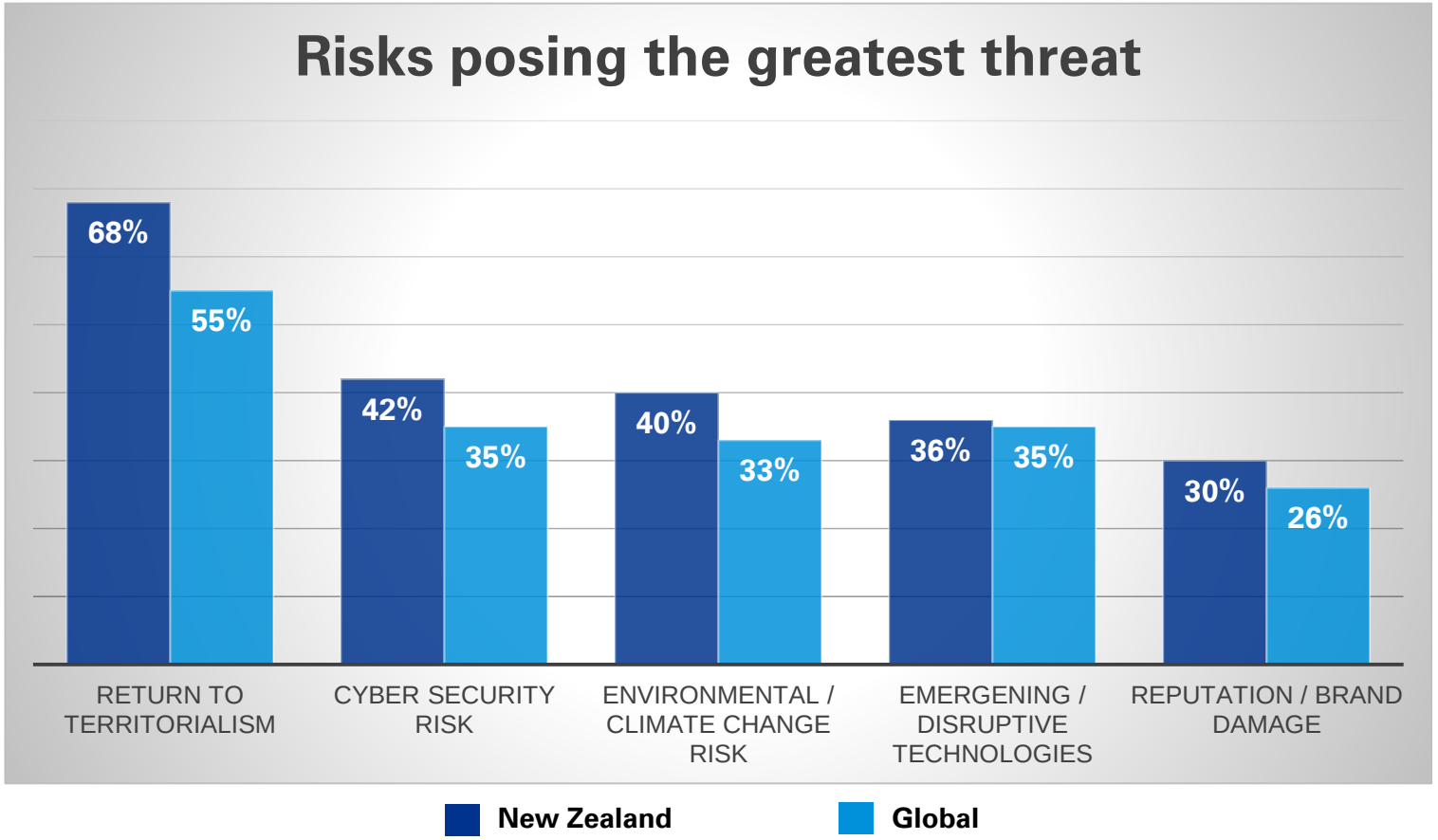
A perspective on the maturity of security in New Zealand

Philip Whitmore
Partner, Cyber Security Services

October 2018

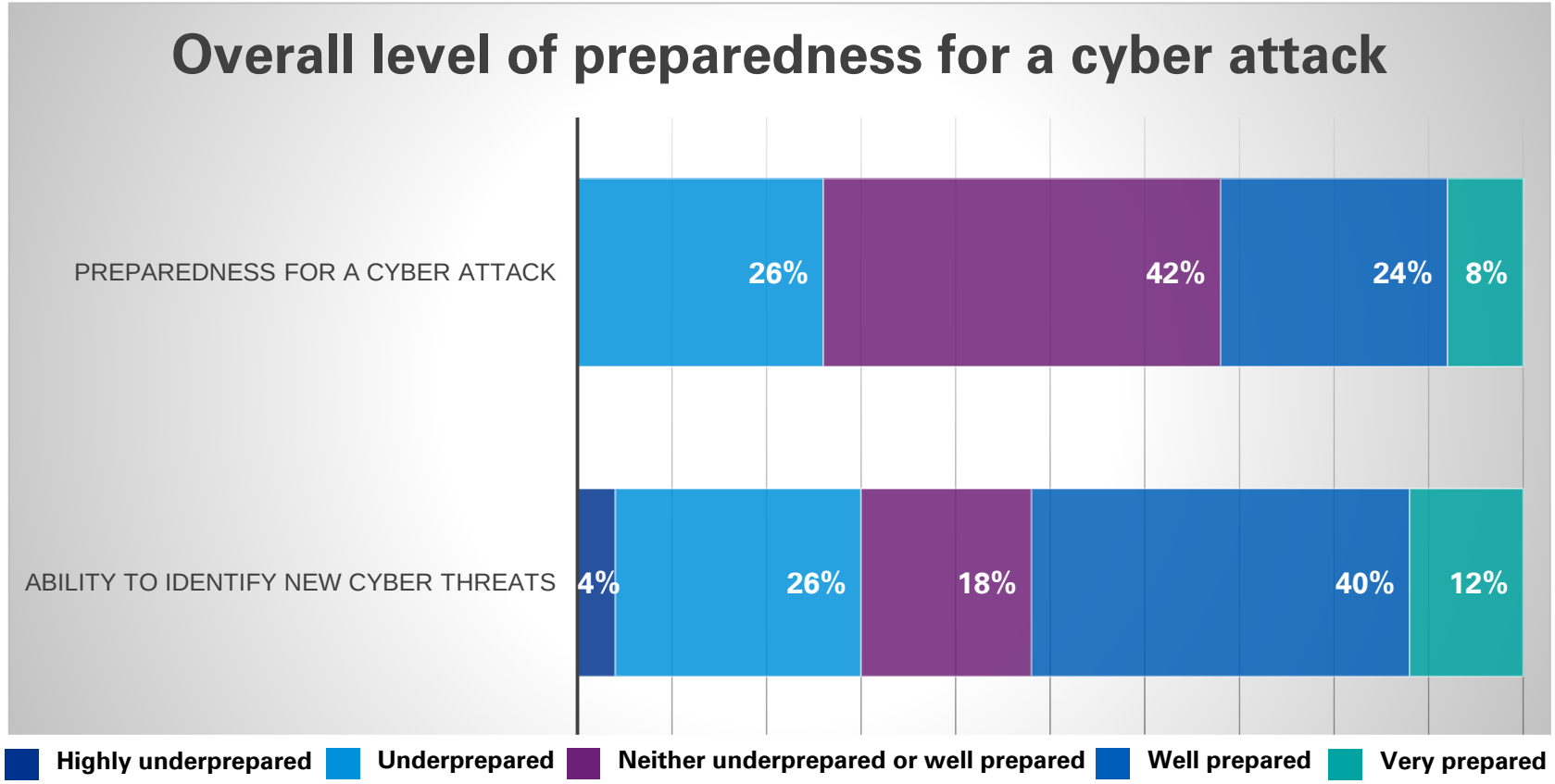
A perspective on the maturity of security in New Zealand

Cyber security continues to be seen in the top three business risks for New Zealand organisations.



KPMG 2018 CEO Outlook – New Zealand, June 2018

A perspective on the maturity of security in New Zealand



KPMG 2018 CEO Outlook – New Zealand, June 2018

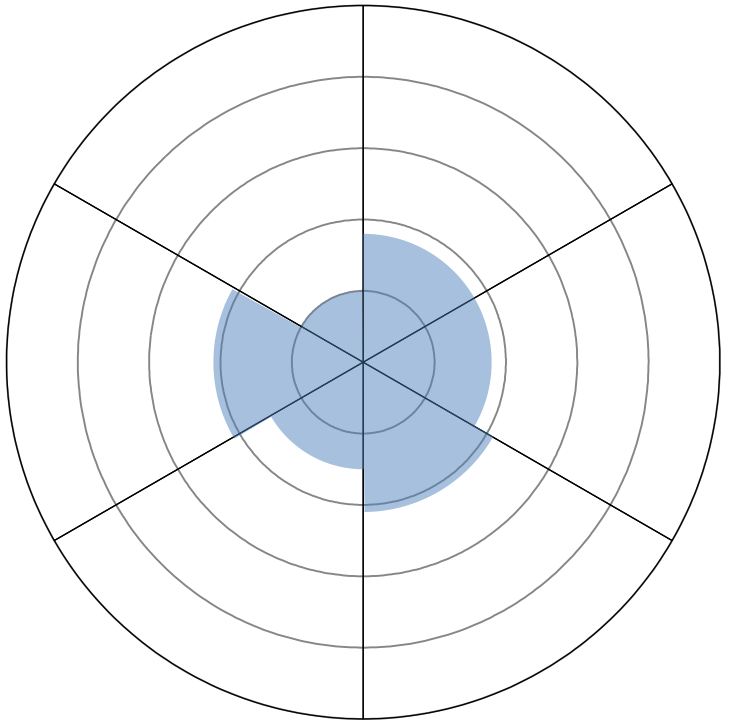
74% of New Zealand organisations consider themselves reasonably well prepared for a cyber attack.

70% believe they have the ability to identify new threats reasonably well.

A perspective on the maturity of security in New Zealand

A perspective on the maturity of security in New Zealand

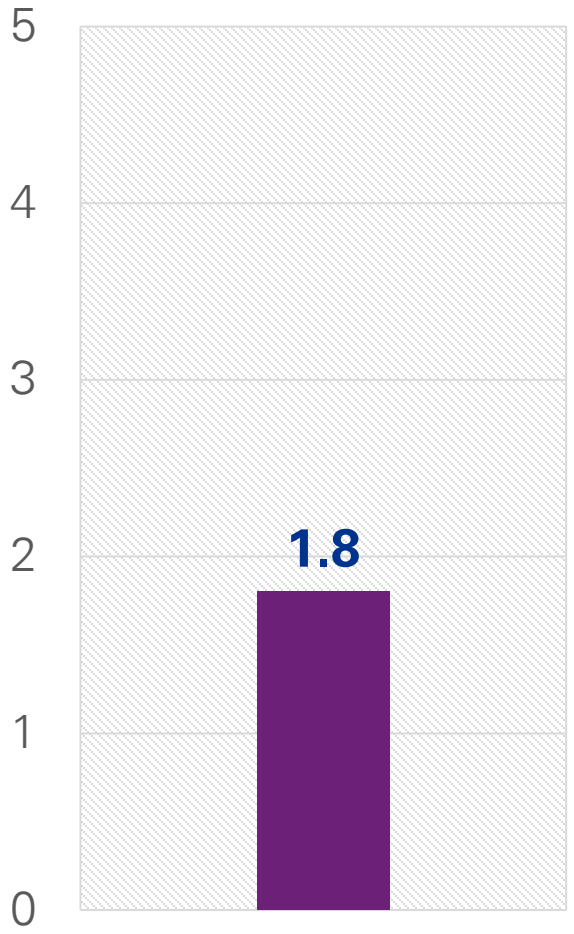
The average maturity of New Zealand organisations is 1.7



A perspective on the maturity of security in New Zealand

Level	Description
0	NON-EXISTENT **Processes are not in place at all**
1	INITIAL **Ad-hoc, unpredictable, poorly controlled, reactive**
2	REPEATABLE **Basic processes, repeatable tasks**
3	DEFINED **Defined and documented processes, proactive**
4	MANAGED **Processes integrated, measured and controlled**
5	OPTIMISED **Continual improvement, organisational alignment**

Leadership and governance



Leadership and governance: Understanding of cyber security, ownership, roles and responsibilities, and direction from the top.

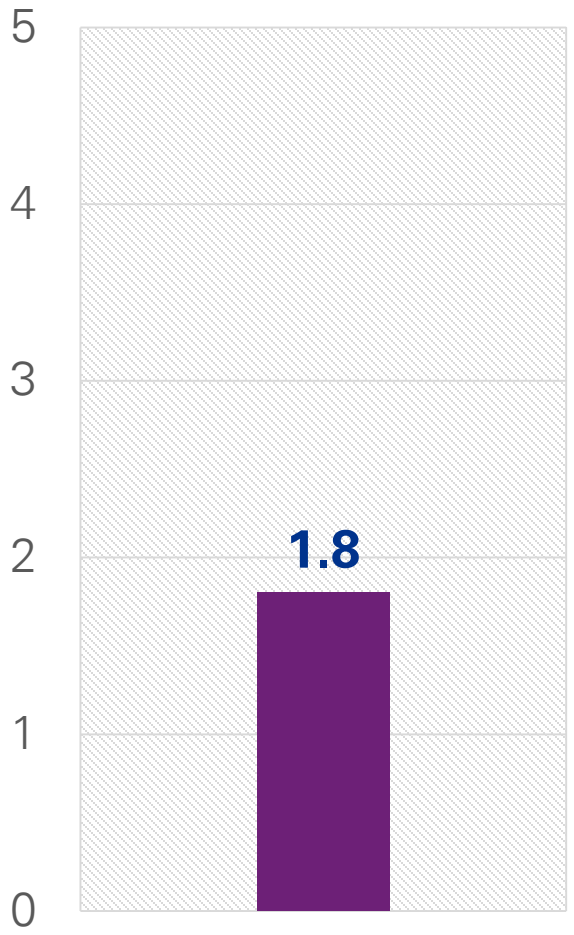
Areas of good practice commonly seen

— Cyber security is recognised by senior management and the Board as a key area of risk.
— A security policy has been developed.
— Security responsibilities are allocated.

Key opportunities

— Appoint a single person as the IT Security Manager (ITSM).
— Establish a structured process to provide the Board and senior management visibility over cyber security.
— Develop detailed security standards and procedures.
— Develop an organisational cyber security strategy.

Human factors



Human factors: The level and integration of a security culture that empowers and ensures the right people, skills, culture and knowledge.

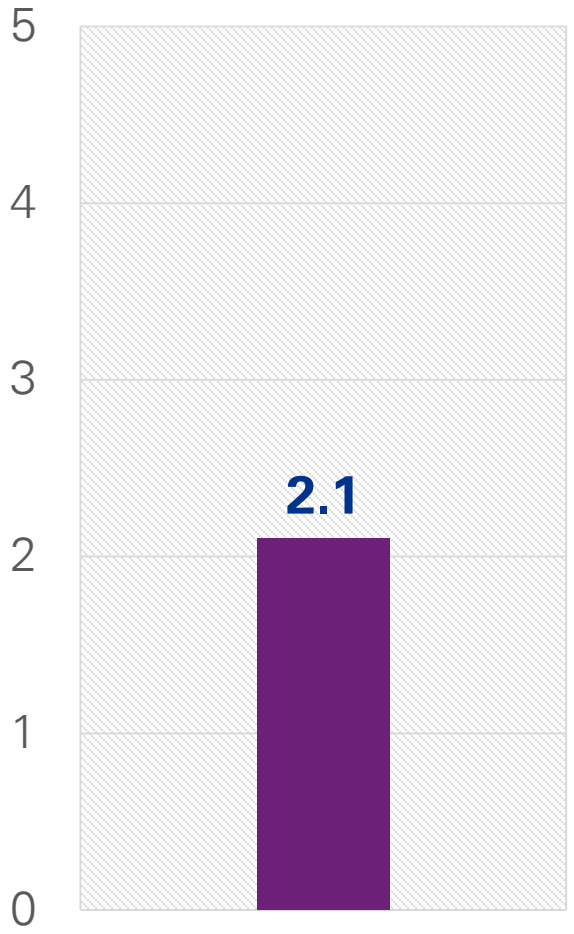
Areas of good practice commonly seen

— General security awareness training is undertaken by all employees when they join an organisation.
— Informal self-training is on security issues is undertaken by IT staff.

Key opportunities

— Establish a security awareness programme and providing security training throughout the year.
— Implement a specialist security training programme for IT staff.
— Actively track completion of security awareness training.
— Treat contractors the same as employees.

Security risk management



Security risk management: The approach to achieve comprehensive and effective security risk management throughout the organisation and its third party providers.

Areas of good practice commonly seen

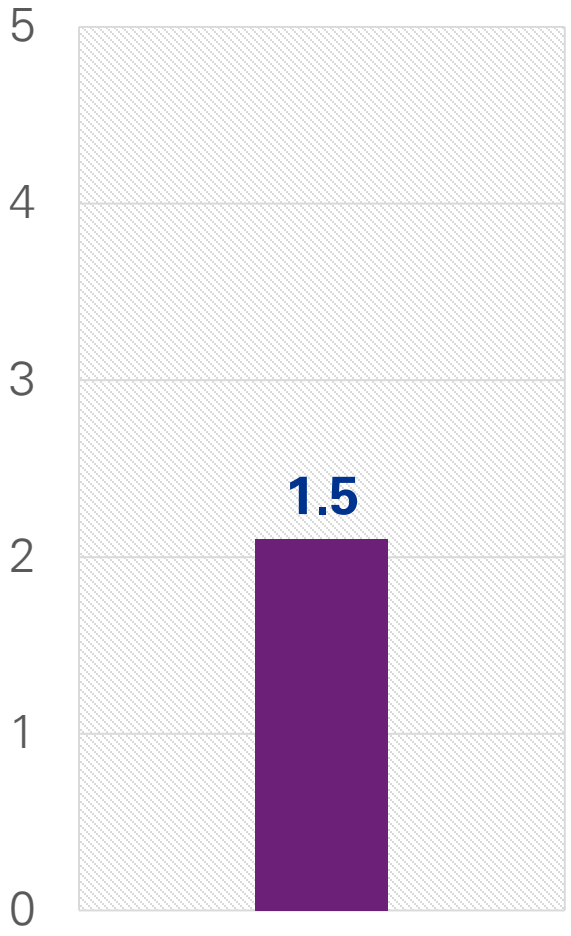
— Security risks are considered are part of the wider organisation risks.
— An asset management process is in place for hardware and software assets.

Key opportunities

— Implement a structured security risk management process.
— Perform security assurance activities over third parties.
— Ensure the IT project methodology considers security throughout the project lifecycle.
— Establish a certification and accreditation process.
— Define the organisation's security risk appetite.

Business continuity

Business continuity: Preparations for a security event and ability to prevent or minimise the impact through successful crisis and stakeholder management.



Areas of good practice commonly seen

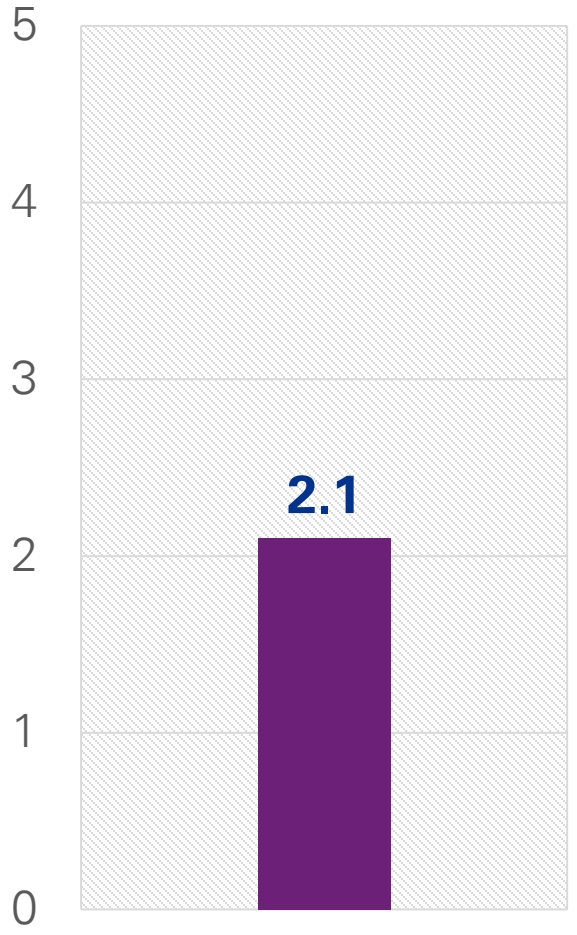
— Key systems are backed up.
— A disaster recovery plan is in place.
— Resilience has been built into key systems.

Key opportunities

— Regularly test the disaster recovery plan and the ability to restore from backups.
— Develop and test a business continuity plan.
— Establish a security incident response process, supported by the appropriate technologies, play books and third party relationships.

Operations and technology

Operations and technology: The level of control measures implemented to address identified risks and minimise the impact of a compromise.



Areas of good practice commonly seen

— Security vetting checks are performed for all employees.
— IT systems are physically secured.
— A structured process is followed for granting access to systems.
— Annual penetration testing is performed.
— Anti-malware software is in place.

Key opportunities

— Establish a formal vulnerability management process.
— Implement a structured logging process.
— Integrate formal checkpoints into systems development and procurement processes.
— Address patching beyond the Windows operating system.
— Implement two-factor authentication for all remote access points.

Legal and compliance

Legal and compliance: Compliance with regulatory, legislative and contractual requirements, as well as gaining assurance that the key security controls align with the risks presented, and continue to operate as intended.

Areas of good practice commonly seen

— Cyber insurance has been considered.

Key opportunities

— Establish a formal security assurance program to validate the effectiveness of key security controls.
— Formally review and track compliance against legislative, regulatory and contractual requirements.

Thank you

Philip Whitmore
Partner, Cyber Security Services
pwhitmore@kpmg.co.nz

@KPMGNZ_Cyber
www.linkedin.com/showcase/kpmg-cyber
www.kpmg.com/nz/cyber