NZ Cyber Resilience Barometer

2nd Quarter 2020 (Sample)

Introduction:

This report contains a summary of cyber resilience submissions from the previous quarter. We provide a series of graphical summaries, along with analytical comment where relevant.

This report covers the quarter from 1 April to 30 June 2020.

Cyber Resilience by Function and Industry:

In this quarter, we received a most submissions from the 'Education and Training' sector. Submissions were received from 11 sectors.

By Industry, the lowest rated function was 'Identify', and the highest was 'Recover'.

Industry	Identify	Protect	Detect	Respond	Recover
Agriculture, Forestry and Fishing	1.7	1.8	2.7	3.2	3.7
Arts, Recreation and Other Services	1.3	3.8	2.0	2.7	3.7
Construction	2.7	2.7	2.7	2.6	3.3
Education and Training	3.9	2.4	2.7	2.6	3.8
Financial and Insurance Services	3.0	3.3	3.3	3.0	3.0
Health Care and Social Assistance	2.5	3.2	2.3	3.3	3.3
Information Media and Telecommunications	2.4	1.9	3.2	3.3	3.3
Manufacturing	1.9	2.8	2.7	2.8	2.8
Professional, Scientific, Technical, Administrative and Support Services	3.3	2.5	2.3	3.2	2.7
Retail Trade and Accommodation	3.7	3.3	3.3	3.4	3.0
Transport, Postal and Warehousing	1.9	2.8	3.2	3.1	2.2
Total	**2.6**	**2.8**	**2.7**	**3.0**	**3.2**

Cyber Resilience by Category:

In this quarter, the lowest performing categories were equally 'Asset Management, Business Environment and Supply Chain Risk Management' and the highest was 'Communications'.

Category	Score
Asset Management	2.4
Business Environment	2.6
Governance	2.4
Risk Assessment	2.9
Risk Management Strategy	2.6
Supply Chain Risk Management	2.4
Identity Management, Authentication and Access Control	2.9
Awareness and Training	2.9
Data Security	2.7
Information Protection Processes and Procedures	2.7
Maintenance	2.7
Protective Technology	2.8
Anomalies and Events	2.8
Security Continuous Monitoring	2.7
Detection Processes	2.6
Response Planning	2.8
Communications	3.1
Analysis	3.1
Mitigation	3.1
Improvements	2.9
Recovery Planning	3.2
Improvements	3.1
Communications	3.4

NZ Cyber Resilience Barometer

2nd Quarter 2020 (Sample)

About the Barometer:

The NZ Cyber Resilience Barometer is published quarterly. The Barometer contains a summary of the latest trends in how New Zealand Organisations are preparing for a cyber incident. An incident may include a cyber attack, data or privacy breach, or similar.

We'll give you a summary of the five functions of the NIST Cybersecurity Framework (Identify, Protect, Detect, Respond, Recover), along with a deep dive into certain categories. We will also provide industry benchmarks where data is available.

Why do we publish this Barometer? Because we want to keep you up to date with the latest trends in how New Zealand organisations are preparing for the risk of a cyber incident,. That way, you can compare how your organisation is tracking against your peers and better prepare for cyber risks before they become problems.

If you would like to receive a tailored report to compare how your organisation is tracking against the Barometer, please get in touch. Access our Privacy Policy here.

About Incident Response Solutions Limited:

Our Purpose - We help you with specialist forensic, cyber security and crisis management expertise at all stages throughout the incident response lifecycle.

Our Promise - We will provide you with the confidence you require to prepare, respond and recover from forensic and cyber incidents.

Our specialist Forensic Technology expertise includes Computer Forensics, Cybercrime Incident Response, Social Media Analysis and eDiscovery. We have significant experience in providing expert witness reports and in delivering expert witness testimony at trial. Our background includes experience in Law Enforcement (NZ Police) and Big 4 Professional Services.

Campbell McKenzie
Director
Incident Response Solutions Limited
0800 WITNESS
+64 21 779 310
campbell@incidentresponse.co.nz

Share our Barometer: