Spark Health

Data security in health

Have confidence in your organisation's cyber-resiliency by staying ahead of tomorrow's security threats.

sparkhealth.co.nz

Digital transformation in health

Cybersecurity is a complex issue affecting a broad spectrum of New Zealand organisations, and New Zealand society as a whole. A digital transformation is underway across the public and private sectors, and cybersecurity is crucial to ensure this transformation is achievable and sustainable. It is especially relevant when reflecting on the rate of rapid technology adoption across New Zealand's health and disability sector.

Today's technology is providing ease of communications between people and agencies as well as improved access to health information that supports clinical and business workflows. This makes trusted communication between agencies an essential part of healthcare delivery, and a fundamental requirement to enable trust and confidence in our health system.

What's happening in the health sector

The Ministry of Health considers the security and privacy of health information to be of paramount importance within our health and disability system. These expectations are expressed through the Health Information Security Framework (HISF), which is designed to support the security practice of organisations that hold personally identifiable health information, and acts as the benchmark for information security standards across the New Zealand health and disability sector.

Looking ahead, the Ministry has signalled its intent to undertake a substantive assurance work programme to continue to lift the health sector's cybersecurity maturity. Achieving this kind of information assurance requires a holistic approach across an organisation's technologies, processes, practices, and culture so that we can identify what success looks like, and can guide health agencies on a journey towards systemic resilience and protection.

Am I cyber-resilient?

- What is my cybersecurity risk appetite and tolerance?
- What and where are my most critical information assets?
- What are the legal, privacy, and security compliance obligations my organisation must meet?
- Am I confident that our employees can identify fraudulent emails?
- Is my cybersecurity framework based on best practices?
- Am I regularly assessing my vulnerabilities?
- Do we have a recovery plan?

$6.5 MILLION

Estimated financial loss due to malicious cyber activity between 1 April – 30 June 2019 (*Cert NZ*)

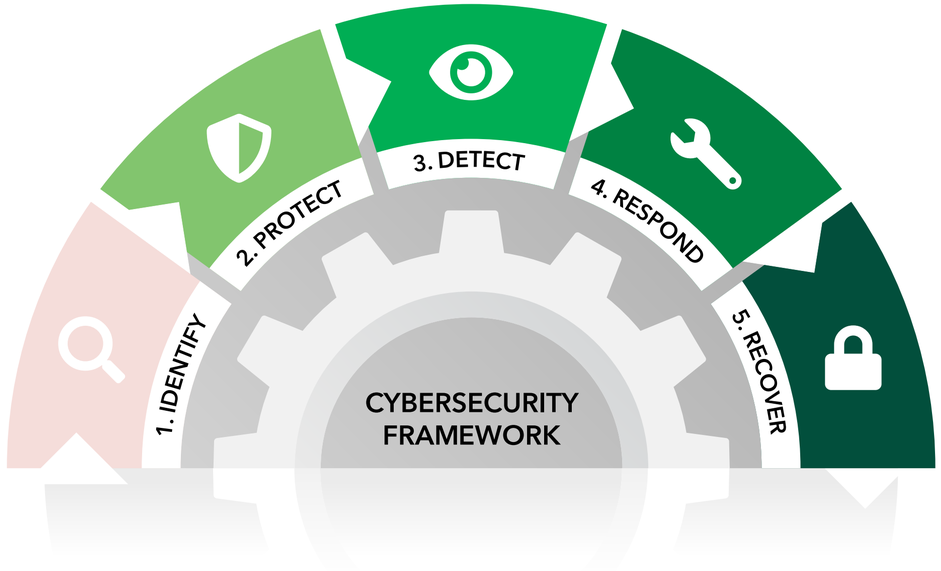
Cybersecurity framework

At Spark Health, we offer a range of security solutions that, when combined, create a robust cybersecurity framework that aligns to local and international best practice. We understand that the health sector requires specialised security compliance requirements, and with the maturity of our security capabilities, we are uniquely placed to support health agencies in all aspects of their cybersecurity journey.

Whether protecting against data loss from environmental catastrophe or from cyber-crime and malware attacks, Spark Health will work with you to meet your desired security posture and risk appetite and strengthen your cyber-resiliency.

A robust cyber-security framework should include the following security control areas:

- **IDENTIFY**
- **PROTECT**
- **DETECT**
- **RESPOND**
- **RECOVER**



1 IDENTIFY

Understand the security posture and risk to your organisation to manage threats before there is a compromise.

- Security Consultancy
- Security Awareness
- Vulnerability Management

2 PROTECT

Protect company assets, data and personal information with technical safeguards and effective cybersecurity awareness training.

- Security Awareness
- Multi-factor & Identity Management
- Endpoint Security
- Mail Security
- Enterprise Security Platform (ESP)

3 DETECT

Implement appropriate measures to quickly identify cybersecurity events and adopt continuous monitoring to detect anamolous activity and other threats to business continuity.

- Endpoint Security Premium
- Enterprise Security Platform (ESP)
- Threat Intelligence

4 RESPOND

Contain the impact of a cyber incident, communicate a response plan, analyse the event, and perform all required activities to eradicate the threat.

- Threat Intelligence
- Professional Services

5 RECOVER

Fully restore any capabilities or services that were impaired due to a cybersecurity event.

- Backup as a Service
- Veeam Cloud Connect
- Disaster Recovery
- Business Continuity Plan
- Professional Services

Our security services

Security Consultancy

Health-sector consulting, HISF benchmarked maturity assessments to identify key risks, practical remediation and roadmap development.

Security ‘thought leadership’, mentoring, ‘virtual’ CISO services, and cybersecurity business-case development support.

Security Awareness

A training platform to simulate realworld security threats with progressive testing and training modules to protect employees against cybersecurity threats as well as user awareness workshops specific to HISF-centric information security.

Vulnerability Management

Identification of software-related security vulnerabilities that exist in an environment with recommended remediation to improve your security posture over time.

Endpoint Security

Fully managed, life-cycle support of anti-virus software.

Mail Security

Mail filtering to stop SPAM and protect against phishing and other mail-based attacks.

Enterprise Security Platform (ESP)

A next-generation security platform that delivers network-based protection against the latest threats.

Threat Intelligence

An advanced detection and response platform that specialises in identifying security breaches that have managed to get past the traditional security controls.

Backup as a Service

A highly scalable and reliable backup infrastructure that protects all levels of your computer system infrastructure.