

# CYBER SECURITY AND RISK MANAGEMENT

An Executive level responsibility





# Cyberspace poses risks as well as opportunities

Cyber security risks are a constantly evolving threat to an organisation's ability to achieve its objectives and deliver its core functions.

Security failings in today's information-driven economy can result in significant long term expense to the affected organisations and substantially damage consumer trust and brand reputation. Sensitive customer information, intellectual property, and even the control of key machinery are increasingly at risk from cyber attack. The targeting of electronic assets has the potential to make a material impact on the entire organisation and possibly its partners.

The topic of cyber security needs to move from being in the domain of the IT professional to that of the Executive and Board, where its consideration and mitigation can be commensurate with the risk posed. The traditional approach to thinking about cyber security in terms of building bigger walls (firewalls and anti-virus software) - while still necessary - is no longer sufficient. A holistic approach to cyber security risk management – across the organisation, its network, supply chains and the larger ecosystem – is required.

**This document provides key questions to guide leadership discussions about cyber security risk management for your organisation. They are intended to be non-prescriptive, as organisational context will vary.**

This publication incorporates work originally researched, drafted and published by our international partners (Australian Defence Signals Directorate, Her Majesty's Government of UK ©Crown Copyright, US-CERT). It has been reproduced with permission and any changes have been made at the discretion of the NCSC. As this publication notes, even well-defended organisations may experience a cyber incident at some point. This publication cannot, and does not, offer any insurance against such incidents. Organisations are urged to seek professional advice in addressing the risks identified here. This publication is not intended to be a substitute for that.

ver 1: 2013

# Protect your reputation

Effective information systems are critical to the success of any organisation. Secure management of intellectual property and confidential or sensitive information provides competitive advantage and helps protect corporate reputation. This is true whether that information is in the form of a product design, a manufacturing process, a negotiating strategy or sensitive personal data. At the same time, the need to access and share information more widely, using a broad range of connecting technologies, increases the risk of that information becoming compromised or misappropriated.

## **COMPROMISE OF INFORMATION ASSETS CAN DAMAGE ORGANISATIONS**

Compromise of information through, for example, staff error or the deliberate actions of an outsider could have a permanent or at least long-term impact on an organisation. A single successful attack could have a devastating impact upon an organisation's financial standing or reputation. Information compromise can lead to material financial loss through loss of productivity, loss of intellectual property, reputational damage, recovery costs, investigation time, and regulatory and legal costs. This in turn could lead to reduced competitive advantage, lower market share, lower profits, adverse media coverage, bankruptcy, or even - where safety-critical systems may be concerned - loss of life.

Boards and Executives need an accurate picture of the information assets critical to an organisation's success. They also need to reassure themselves that they have up-to-date information on the known business security vulnerabilities and threats so they can make informed information risk decisions.



## MANY ACTORS POSE A RISK TO INFORMATION

There are many types of actors who pose a risk to business via IT information assets:

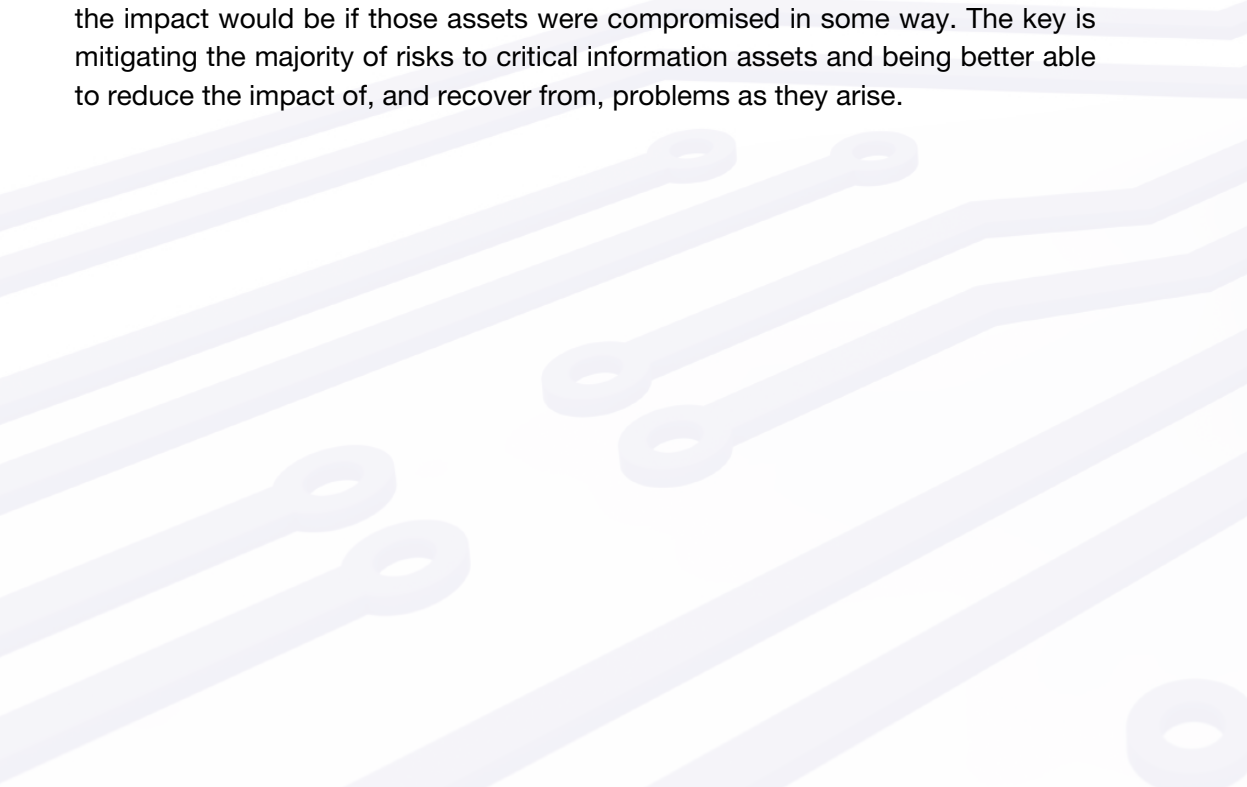
- ▶ cyber criminals interested in making money through fraud or from the sale of valuable information
- ▶ industrial competitors and foreign state actors interested in gaining an economic advantage for their own companies or countries
- ▶ hackers who find interfering with computer systems an enjoyable challenge
- ▶ hacktivists who wish to attack companies for political or ideological motives
- ▶ employees, or those who have legitimate access, either by accident or deliberate misuse.

## THE THREAT IS NOT ONLY TECHNICAL

Many attempts to compromise information involve what is known as “social engineering”, or the skilful manipulation of people and human nature. It is often easier to trick someone into clicking on a malicious link in an email that they think is from a friend or colleague than it is to hack into a system, particularly if the recipient of the email is busy or distracted. There are also many well documented cases of hackers persuading IT support staff to open up areas of a network or reset passwords, simply by masquerading as someone trusted.

## THE KEY IS EFFECTIVE ORGANISATION-WIDE RISK MANAGEMENT AND AWARENESS

Being aware of potential threats is a normal part of risk management across organisations. Alongside financial, legal, HR and other business risks, companies need to consider what could threaten their critical information assets and what the impact would be if those assets were compromised in some way. The key is mitigating the majority of risks to critical information assets and being better able to reduce the impact of, and recover from, problems as they arise.



# Put cyber security on the agenda before it becomes the agenda

## **INCORPORATE CYBER RISKS INTO EXISTING RISK MANAGEMENT AND GOVERNANCE PROCESSES**

Cyber security is NOT implementing a checklist of requirements; rather it is managing cyber risks to an acceptable level. Managing cyber security risk as part of an organisation's governance, risk management, and business continuity frameworks provides the strategic framework for managing cyber security risk throughout the organisation.

## **ELEVATE CYBER RISK MANAGEMENT DISCUSSIONS TO THE EXECUTIVE**

Executive engagement in defining the risk strategy and levels of acceptable risk enables more cost effective management of cyber risks that are aligned with business needs. Regular communication between the CEO and those held accountable for managing cyber risks provides awareness of current risks affecting the organisation and associated business impact.

## **IMPLEMENT INDUSTRY STANDARDS AND BEST PRACTICES, DON'T RELY ON COMPLIANCE**

A comprehensive cyber security programme leverages industry standards and best practices to protect systems and detect potential problems. It is supported by processes informed of current threats and enables timely response and recovery. Compliance requirements help to establish a good cyber security baseline to address known vulnerabilities, but do not adequately address new and dynamic threats, or counter sophisticated adversaries. Using a risk-based approach to apply cyber security standards and practices allows for more comprehensive and cost effective management of cyber risks than compliance activities alone.



## **EVALUATE AND MANAGE YOUR ORGANISATION'S SPECIFIC CYBER RISKS**

Identifying critical assets and associated impacts from cyber threats are key to understanding a company's specific risk exposure— whether financial, competitive, reputational, or regulatory.

Risk assessment results are a key input to identify and prioritise specific protective measures, allocate resources, inform long-term investments, and develop policies and strategies to manage cyber risks to an acceptable level.

## **PROVIDE OVERSIGHT AND REVIEW**

Executives are responsible for managing and overseeing organisation risk management. Cyber oversight activities include the regular evaluation of cyber security budgets, IT acquisition plans, IT outsourcing, cloud services, incident reports, risk assessment results, and top-level policies.

## **DEVELOP AND TEST INCIDENT RESPONSE PLANS AND PROCEDURES**

Even a well-defended organisation will experience a cyber incident at some point. When network defences are penetrated, an organisation should have a clear idea of how to respond. Documented cyber incident response plans that are exercised regularly help to enable timely response and minimise impacts.

Coordinate cyber incident response planning across the organisation. Early response actions can limit or even prevent possible damage. A key component of cyber incident response preparation is planning in conjunction with the entire executive, business leaders, continuity planners, system operators, general counsel, and public affairs. This includes integrating cyber incident response policies and procedures with existing disaster recovery and business continuity plans.

## **MAINTAIN SITUATIONAL AWARENESS OF CYBER THREATS**

Situational awareness of an organisation's cyber risk environment involves timely detection of cyber incidents along with an awareness of current threats and vulnerabilities specific to the organisation and associated business impacts. Analysing, aggregating, and integrating risk data from various sources and participating in threat information sharing with partners helps organisations identify and respond to incidents quickly and ensure protective efforts are commensurate with risk.

A network operations centre can provide real-time and trend data on cyber events. Business-line managers can help identify strategic risks, such as risks to the supply chain created through third party vendors or cyber interdependencies. Sector Information-Sharing and Analysis Centres, government and intelligence agencies, academic institutions, and research firms also serve as valuable sources of threat and vulnerability information that can be used to enhance situational awareness.

# Ten steps to reduce your cyber risk

Basic information risk management has been shown to prevent up to 85% of the cyber attacks seen today, allowing organisations to concentrate on managing the impact of the other 15%. Organisations should take steps to review, and invest where necessary, to improve security in the following key areas:

<b>Information Risk Management Regime</b>	Establish an effective governance structure and determine your risk appetite - just like you would for any other risk. Maintain the Board's engagement with the cyber risk. Produce supporting information risk management policies.
<b>Home and Mobile Working</b>	Develop a mobile working policy and train staff to adhere to it. Apply the secure baseline build to all devices. Protect data both in transit and at rest.
<b>User Education and Awareness</b>	Produce user security policies covering acceptable and secure use of the organisation's systems. Establish a staff training programme. Maintain user awareness of the cyber risks.
<b>Incident Management</b>	Establish an incident response and disaster recovery capability. Produce and test incident management plans. Provide specialist training to the incident management team. Report criminal incidents to law enforcement.
<b>Managing User Privileges</b>	Establish account management processes and limit the number of privileged accounts. Limit user privileges and monitor user activity. Control access to activity and audit logs.
<b>Removable Media Controls</b>	Produce a policy to control all access to removable media. Limit media types and use. Scan all media for malware before importing on to corporate system.
<b>Monitoring</b>	Establish a monitoring strategy and produce supporting policies. Continuously monitor all ICT systems and networks. Analyse logs for unusual activity that could indicate an attack.
<b>Secure Configuration</b>	Apply security patches and ensure that the secure configuration of all ICT systems is maintained. Create a system inventory and define a baseline build for all ICT devices.
<b>Malware Protection</b>	Produce relevant policy and establish anti-malware defences that are applicable and relevant to all business areas. Scan for malware across the organisation.
<b>Network Security</b>	Protect your networks against external and internal attack. Manage the network perimeter. Filter out unauthorised access and malicious content. Monitor and test security controls.

# Next steps

If you are uncertain about your organisation's ability to manage its information risks, here are some practical steps that can be taken through corporate governance mechanisms:

1. Confirm that you have identified your key information assets and the impact on your business if they were to be compromised.
2. Confirm that you have clearly identified the key threats to your information assets and set an appetite for the associated risks.
3. Confirm that you are appropriately managing the cyber risks to your information and have the necessary security policies in place.

Companies may not have all the expertise needed to implement some of these steps and assure themselves that the measures they have in place meet today's threats. Audit partners should be able to provide assistance in the first instance. For information risk management expertise, organisations should seek advice from members of appropriate professional bodies or those who have attained industry recognised qualifications.



## ABOUT NCSC

The National Cyber Security Centre (NCSC) is responsible for safeguarding our nation's government and critical infrastructure from cyber-borne threats that can affect our national security, public safety, and economic prosperity.

For more information, please visit: [www.ncsc.govt.nz](http://www.ncsc.govt.nz)

To report a cyber incident: [www.ncsc.govt.nz/incidents](http://www.ncsc.govt.nz/incidents) or +64 4 498 7654