Cyber Security: guidance

Introduction

Cyber security is an integrated approach to preparing for, protecting against, detecting and responding to cyber threats; it is not just a technical issue. Cyber security refers to the technologies, processes and practices, both digital and human, designed to protect IT networks, programs and data from attack, damage, compromise or unauthorised access. It also covers the identification of and recovery from disruptions following cyber-attacks.

Technological advances and the globalisation of the supply chain create opportunities for greater government efficiency and effectiveness. These include new ways to work remotely and to store and transfer data, such as mobile devices and cloud computing. As employees spend more time away from the office using a variety of IT applications and access arrangements, the dramatic increase in the flow of information in and out of the organisation becomes more difficult to control and this presents more opportunities for attackers.

Cyber security is now a key issue for most boards and senior executives and non-executives are becoming more pre-emptive in evaluating cyber security risk exposure as an enterprise-wide risk management issue and not limiting it to an IT concern. Senior management will continue to play a fundamental role in understanding the risks associated with cyber security and confirming preventative and detective controls are in place.

The NCSC's Cyber Security Toolkit for Boards is a dedicated resource designed to encourage essential cyber security discussions between the Board and their technical experts. It provides an introduction to key areas of cyber security as well as a set of questions an organisation can use to support cyber security governance. Topics include understanding the cyber security threat, collaborating with suppliers and partners and preparing your response to a cyber incident.

Cyber threat

Cyber threat actors can be grouped into the following:

1) Cyber criminals – they will target any organisation large or small. They might try and steal money; hold systems and information to ransom; or try and steal sensitive data that they can sell on. The term cyber criminals covers a wide range of people from self-taught amateurs to highly resourced and organised criminal groups.

2) Hostile foreign governments – they normally have a more specific target in mind and are not usually motivated by money, but more likely they will be aiming to acquire sensitive information that could provide a political or strategic advantage, to steal intellectual property that provides economic advantage, or test the defences of their targets.
3) Activists -who want to prove a point for political or ideological reasons, for instance to expose or discredit an organisation's activities.
4) Terrorists – interested in spreading propaganda and looking to disrupt activities.
5) Insiders – employees or recent leavers, who may have extensive access to sensitive information, networks or systems. An insider could be someone carrying out sophisticated corporate espionage or it could simply be a disgruntled employee.

Cyber threat and attacks can come in various forms:

- A common form of cyber-attack against government is the use **of false or stolen customer credentials to commit fraud**. The uptake in online services means this form of crime can now be done on a much larger scale and foreign nationals can defraud government organisations from outside the UK. One way of reducing the risk of fraud is by using multi-factor authentication, which makes it harder for criminals to access online accounts even if they know the password.
- Cyber criminals seek to **steal data from government networks that has a value on the black market**, e.g. financial information or data that can be used for ID theft. Several types of malware have been specifically designed by cyber criminals to exploit e-banking details or log-in information. Such malware is sometimes found on government networks, but financial and commercial organisations are more likely to be targeted.
- Cyber criminals seek to **control computer infrastructure** and use it as a platform for carrying out other activity such as sending spam and phishing emails. Government networks are an attractive target.
- These groups also launch **ransom attacks**, locking victims out of their data and only providing the 'key' once money is paid. Ransomware has been a growing cyber security threat, and one which could affect any organisation that does not have appropriate defences.
- Recently, more targeted ransomware attacks have become common, in which victim networks are analysed to understand their 'value' and ransom demands set based on that perceived value. Criminal actors also seek to ensure that their malicious activity has the maximum impact on the victim organisation – potentially **denying the victim access to business-critical files and systems and disrupting the operations** of the victim organisation. Attackers will also threaten to publish data if payment is not made.
- Several of the most sophisticated and hostile foreign intelligence agencies target UK government networks to **steal sensitive information**. This could ultimately disadvantage the UK in diplomatic or trade negotiations, or militarily.
- Also, hacktivists, insiders and terrorists pose a cyber threat: **hacktivists** crave publicity and for them, success is causing embarrassment or annoyance to the owners of high-profile websites and social media platforms that they deface or take offline. When targeted against government websites and networks, these attacks can cause reputational damage to the UK at home and abroad.
- An **insider** is someone who exploits, or intends to exploit, their legitimate access to an organisation's assets for unauthorised purposes. Such activity can include unauthorised disclosure of sensitive information, facilitation of third party access to an organisation's assets, physical sabotage and electronic or IT sabotage.

- Some **terrorist** groups demonstrate an intent to conduct cyber-attacks. The sharing of expertise in online forums provides a significant opportunity for terrorists to escalate their capability.

Role of Audit and Risk Assurance Committee

Audit and risk assurance committees' (ARAC) role is to provide assurance to the Board that the organisation is properly managing its cyber risk including appropriate risk mitigation strategies. This does not necessitate understanding the full detail of the technology involved; ARAC can confirm that the appropriate framework is in place and that continuous monitoring and improvement initiatives are adopted and sustained. It is important to understand the organisation's tolerance for risk and evaluate the risk decisions made by management. Exploring opportunities to share information and to use technology should be guided by the organisation's risk appetite.

In particular, to assess the organisation's cyber resilience the ARAC should evaluate whether the organisation has:

Governance

- controls in place to prepare for, protect from, detect and respond to cyber-attacks including management of the consequences of a cyber-security incident;
- a means of monitoring the effectiveness of their cyber security controls, including where appropriate, independently testing, reviewing and assuring such controls;
- identified the critical information assets which it wishes to protect against cyber attack and who is responsible for them – whether financial data, operational data, employee data, customer data or intellectual property;
- a way of identifying and agreeing the level of risk of cyber-attack that the organisation is prepared to tolerate for a given information asset (What level of cyber security risk is considered acceptable?);
- an operational risk framework and internal audit plan providing cover across different areas of cyber security, not just focused on IT operations;

Threat Intelligence; Third Party and Supply Chain

- an understanding of what data is leaving the organisation and its destination, and what associated monitoring activities are in place;
- intelligence processes in place to understand the threat to the organisation's assets including a detailed understanding of which suppliers/partners connect to the organisation and how experienced;
- an increase in the number of information security breaches;

Structure and Resources

- the right skills and experience in-house to cover all relevant areas;
- the right management structure in place, including the Senior Information Risk Owner (SIRO);

Business Continuity

- established a disaster recovery plan in case of loss of critical data (e.g. through a ransomware incident);
- regularly extracted and stored system backups in an offline environment;
- tested and assured system backups for consistency and reliability;

Incident Response

- an up-to-date response plan for cyber incidents which has been practiced including actions on lessons learnt;

People, Training and Awareness

- training and awareness programmes to educate the workforce about cyber risks and individual responsibilities;
- a programme of continuous improvement, or where needed, transformation, to match the changing cyber threat with appropriate performance indicators

The ARAC could consider using the organisation's SIRO to provide assurance over these and other issues by:

- getting regular briefs at ARAC meetings from the SIRO, including progress on the maturity of the organisation in information risk and cyber security
- reviewing an annual report from the SIRO as part of the financial year end assurance process, and discussing with the SIRO any issues that the ARAC should include in its recommendation for the Governance Statement

A further option for the ARAC is to consider whether one of its members could become a champion on cyber security at the ARAC (and the Board if a member), and support the SIRO.

Related Resources from the National Cyber Security Centre (NCSC) and other organisations

The Cyber Security Toolkit for Boards

The NCSC's Cyber Security Toolkit for Boards includes questions that Board members can use to seek assurance over their organisation's approach to cyber security and encourage essential cyber security discussions between the Board and their technical experts.

https://www.ncsc.gov.uk/collection/board-toolkit

Ten Steps to Cyber Security

The Ten Steps to Cyber Security is designed to help organisations protect themselves in cyberspace. It breaks down the task of defending your networks, systems and information into its essential components, providing advice on how to achieve the best possible security in each of these areas.

The 10 steps to cyber security was originally published in 2012 and is now used by a majority of the FTSE350.

https://www.ncsc.gov.uk/collection/10-steps-to-cyber-security

The Cyber Essentials Scheme

Cyber Essentials is a simple but effective, Government backed scheme that will help you to protect your organisation, whatever its size, against a whole range of the most common cyber attacks.

Cyber attacks come in many shapes and sizes, but the vast majority are very basic in nature, carried out by relatively unskilled individuals. They're the digital equivalent of a thief trying your front door to see if it's unlocked. The advice within Cyber Essentials is designed to prevent these attacks.

https://www.ncsc.gov.uk/cyberessentials/overview

Cyber Incident Response

This guidance collection will help you plan, build, develop and maintain an effective cyber incident response capability.

https://www.ncsc.gov.uk/collection/incident-management

Cyber-Security Information Sharing Partnership (CISP)

CISP is a forum for cyber security discussion from beginner through to expert level, managed by the NCSC. It's also a platform where organisations can share intelligence gathered from their own computer networks.

https://www.ncsc.gov.uk/section/keep-up-to-date/cisp

Certified Cyber Security Consultancy

Independently certified, industry delivered, consultancy for government, wider public sector and Critical National Infrastructure organisations.

https://www.ncsc.gov.uk/information/ncsc-certified-cyber-security-consultancy

The National Cyber Crime Unit (NCCU)

The NCCU, as part of the National Crime Agency (NCA), is the UK lead for the investigation of the most serious and organised cybercrime. The NCCU will support domestic and international law enforcement, and the wider NCA, to take responsibility for tackling cyber and cyber-enabled crime affecting the UK.

The NCCU will be accessible to partners; responding dynamically to threats, providing expert advice, guidance and feedback. The NCA is not a crime reporting agency, so any reports of crime should be reported to Action Fraud (see below).

www.nationalcrimeagency.gov.uk

Action Fraud

Action Fraud is the UK's single point for reporting all fraud and online financial crime. Crime can be reported online 24 hours a day, seven days a week, and the Action Fraud call centre can also be contacted to report crimes during working hours and at the weekend. When a serious threat or new

type of fraud is identified, Action Fraud will place an alert on its website which contains advice for individuals and businesses to protect themselves from becoming victims of fraud.

www.actionfraud.police.uk

Centre for the Protection of National Infrastructure (CPNI)

CPNI protects national security by providing protective security advice, covering physical, personnel and cyber security, to the UK's Critical National Infrastructure (CNI). CPNI works to raise awareness at board level as well as at a technical level across the CNI. Cyber security advice and guidance is available on the CPNI website.

www.cpni.gov.uk