Executive Companion

CESG
The Information Security Arm of GCHQ

10 Steps to Cyber Security

BIS Department for Business Innovation & Skills

CPNI Centre for the Protection of National Infrastructure

CabinetOffice Office of Cyber Security & Information Assurance

CESG
The Information Security Arm of GCHQ

Executive Companion

Content

Foreword

Every day, all around the world, thousands of IT systems are compromised. Some are attacked purely for the kudos of doing so, others for political motives, but most commonly they are attacked to steal money or commercial secrets. ***Are you confident that your cyber security governance regime minimises the risks of this happening to your business?*** My experience suggests that in practice, few companies have got this right.

And if your company doesn't have it right, your IT systems may have already been compromised, attackers could already have your new product plans, bidding positions or research; they may already be running your process control systems. ***Are you confident that this has not already happened to your business?***

Whatever business we are in, we all rely on the internet. We research and develop on it; bid and sell on it; communicate with our customers on it and rely upon it for our logistical support. Put simply, the internet brings immeasurable benefits. But, we cannot escape the fact that it also brings new risks.

About 80 per cent of known attacks would be defeated by embedding basic information security practices for your people, processes and technology. ***This guidance is about getting those basics right;*** where companies adopt these steps it has made a tangible difference to their vulnerability to cyber attack.

My organisation, GCHQ, now sees real and credible threats to cyber security of an unprecedented scale, diversity and complexity. We've seen determined and successful efforts to:

- steal intellectual property;
- take commercially sensitive data, such as key negotiating positions;
- access government and defence related information;
- disrupt government and industry service; and,
- exploit information security weaknesses through the targeting of partners, subsidiaries and supply chains at home and abroad.

The magnitude and tempo of these attacks, basic or sophisticated, on UK and global networks pose a real threat to the UK's economic security. The mitigation of these risks and management of these threats - in other words, cyber security - is one of the biggest challenges we all face today.

Many different groups may pose a threat to a company's information assets: criminals interested in making money through fraud, operating not just as individuals but often in well-organised groups based in hard-to-reach jurisdictions; industrial competitors and foreign intelligence services interested in gaining competitive advantage for their own companies or countries; hackers who revel in the challenge of penetrating and disrupting computer systems and hacktivists who cause disruption for political or ideological reasons. And the insider threat should not be overlooked: potentially the actions of a company's own employees pose a risk, whether careless or malicious.

The technical level of cyber attacks is growing exponentially. What was considered a sophisticated cyber attack only a year ago might now be incorporated into a downloadable and easy to deploy internet application, requiring little or no expertise to use.

Responsibility to manage your company's cyber risks starts and stops at Board level. You can never be totally safe. Risks will, at times, become reality. To that end this guidance is designed to offer some practical steps which you, as leaders, can direct to be taken to improve the protection of your networks and the information carried upon them. ***Value, Revenue and Credibility are at stake. Don't let cyber security become the agenda - put it on the agenda.***

Iain Lobban
Director GCHQ

Cyberspace Poses Risks As Well As Opportunities

What is Cyberspace?

"Cyberspace is an interactive domain made up of digital networks that is used to store, modify and communicate information. It includes the internet, but also the other information systems that support our businesses, infrastructure and services."

UK Cyber Security Strategy, 2011

Common usage of the term also refers to the virtual environment of information and interactions between people.

Information is critical to today's business

Information and the ICT (Information and Communication Technologies) that store and process it are critical to business success. Your intellectual property, confidential or sensitive information provide competitive advantage, whether in the form of a product design, a manufacturing process or a negotiating strategy. At the same time the need to access and share information more widely, using a broad range of connecting technologies is increasing the risk to the corporate information base.

Compromise of information assets can damage companies

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 a business. A single successful attack could destroy a company's financial standing or reputation. Information compromise can lead to material financial loss through loss of productivity, of intellectual property, reputational damage, recovery costs, investigation time, regulatory and legal costs. This could lead to reduced competitive advantage, lower market share, impact on profits, adverse media coverage, bankruptcy, or even, where safety-critical systems may be concerned, loss of life.

In addition to an accurate picture of those information assets that are critical to business success, Boards will wish to reassure themselves that they have regular up to date information on the threats and known business vulnerabilities to make informed information risk decisions.

We can all name companies whose cyber security has been very publicly compromised: where it has happened, this has caused tangible damage. ***What makes your business immune to such attacks?***

Many players pose a risk to information

There are many types of people who pose a risk to business information assets:

- **cyber criminals** interested in making money through fraud or from the sale of valuable information;
- **industrial competitors** and **foreign intelligence services**, 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. And there are 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 else over the phone.

The key is effective enterprise-wide risk management and awareness

Being aware of potential threats is a normal part of risk management across the private sector. 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.

What is information?

Information, whether financial or about people and systems, is the lifeblood of any organisation. Yet, with increasing automation and interconnectivity of information systems, a compromise in one area could impact the entire organisation and its customers. Information is everywhere from customer facing systems (ATMs, points of sale, mobile phones), to business systems (research data and other intellectual property, management and customer relationship information) and operational systems (safety, protection, process control). When identifying information assets, all of these different areas need to be taken into consideration.

Put Cyber Security On The Agenda Before It Becomes The Agenda

A major cyber attack may feel like the stuff of popular culture. It's not. Although many never hit the headlines, such attacks are increasing in prevalence and scale all the time. The impact of not recognising and pre-empting cyber risks can be long term.

Risks to all forms of information should be treated in the same way as other financial or business risks, especially where threats and vulnerabilities are constantly changing. Ultimate responsibility for cyber security rests at Board level, with the correct governance, management and culture throughout the business. The Board should seek assurance that key information risks are both assessed and prioritised, and that there is regular monitoring where threats and vulnerabilities are constantly changing. The Board should also set the value the company places on its various information assets such as company pricing data, business strategies, online services and process control systems, and communicate this throughout the business.

What information should you protect?

All business activity relies on information in a number of forms; it may be supporting corporate management decisions, user access to information, operational networks or process control systems. Review your information assets and agree which are the most critical to the success and competitive advantage of your company.

What are the risks to your information and how much risk can you accept?

Identify the risks to information assets. Assess who has access to those assets and who may wish to target the company. Consider the circumstances in which the risks have or could become a reality. Quantify the level of risk to those assets that the business is willing to accept and communicate your risk appetite across the business, especially to those who implement and manage the company's security. Ensure your assessments keep pace with technological advances, such as Cloud Computing, which may affect the balance of risk over time.

What measures do you need?

Ensure that your governance framework encompasses information risk across the business and apply the same degree of rigour to these risks as financial and other risk management regimes. Implement security controls and supporting policies that are commensurate with the level of risk that the business is willing to tolerate. To support this process we have set out at page 8, ten steps that support a robust information risk and cyber security regime. If any of these areas are not covered in your framework, is there a sound business rationale?

Do the security measures work?

Regularly review and test the effectiveness of, and adherence to, current controls, and investigate any anomalies. Often well intentioned policies believed to be critical to preventing disaster are not being followed in practice. This could be down to a lack of training, a culture of complacency or simply because they are not usable.

What would happen to the business if one of your risks became a reality?

Plan for a worst case scenario. Have robust, regularly tested, incident management processes and contingency planning in place to recover from and reduce the impact of any compromises to the business. Understanding why an attack occurred and what was compromised is critical to recovering successfully and protecting the business in the future.

How do you embed risk management within your company?

Effectively managing the process of assessing risks and implementing controls is essential - both in the business and supply chain. The appropriate people need to be accountable for information and its protection, and should have the right authority, tools and training to achieve this.

How can you ensure that you have the best possible understanding of the threat to your business?

Empower selected senior staff to share appropriate information with others in your and related business sectors, both to help build best practice and warn of potential upcoming attacks. Report crime to Action Fraud or other relevant agencies to help law enforcement build a fuller picture of the threat to business, share the findings and deploy appropriate support.

Ten Steps to Reduce Your Cyber Risk

Basic information risk management can stop up to 80% of the cyber attacks seen today, allowing companies to concentrate on managing the impact of the other 20%. We recommend that as a business you take steps to review, and invest where necessary, to improve security in the following key areas:

Home & Mobile Working

Develop a mobile working policy & train staff to adhere to it. Apply the secure baseline build to all devices. Protect data both in transit & at rest.

User Education & Awareness

Produce user security policies covering acceptable & secure use of the organisation's systems. Establish a staff training programme. Maintain user awareness of the cyber risks.

Incident Management

Establish an incident response & disaster recovery capability. Produce & test incident management plans. Provide specialist training to the incident management team. Report criminal incidents to law enforcement.

Information Risk Management Regime

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.

Managing User Privileges

Establish account management processes & limit the number of privileged accounts. Limit user privileges & monitor user activity. Control access to activity & audit logs.

Removable Media Controls

Produce a policy to control all access to removable media. Limit media types & use. Scan all media for malware before importing on to corporate system.

Monitoring

Establish a monitoring strategy & produce supporting policies. Continuously monitor all ICT systems & networks. Analyse logs for unusual activity that could indicate an attack.

Secure Configuration

Apply security patches & ensure that the secure configuration of all ICT systems is maintained. Create a system inventory & define a baseline build for all ICT devices.

Malware Protection

Produce relevant policy & establish anti-malware defences that are applicable & relevant to all business areas. Scan for malware across the organisation.

Network Security

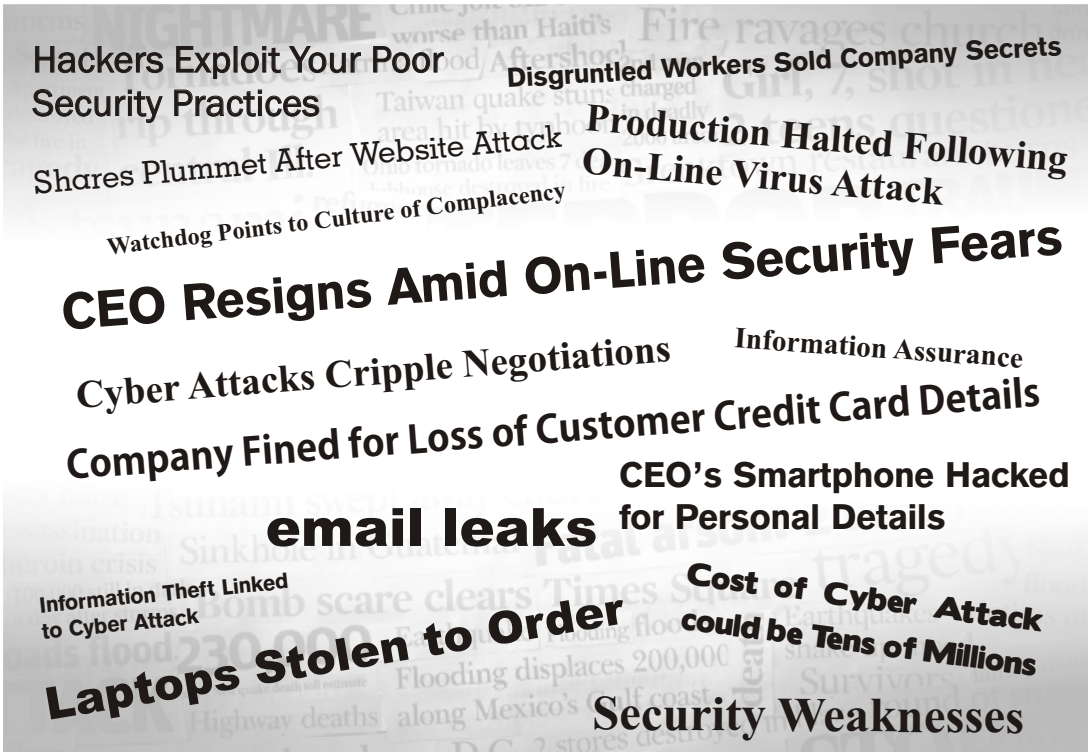
Protect your networks against external and internal attack.Manage the network perimeter. Filter out unauthorised access & malicious content. Monitor & test security controls.

Be a hard target - learn from others

Many companies across different industry sectors will already have experienced some form of cyber attack. Whilst the scenarios on the following pages are illustrative, they are based on events that had real impact on the companies that experienced them. They are just three examples of the many hundreds of incidents we see occurring regularly. Application of the 10 steps provides a comprehensive information risk management framework; however, for each scenario we have suggested those of particular relevance.

The suggested cyber controls in this booklet cannot prevent all of the most sophisticated cyber attacks, but they can greatly hinder the vast majority of attackers; reduce the vulnerability of a particular company; and limit any impact in the event of a breach. Engagement with peers across your sector, the wider business community and law enforcement can help you to maintain an understanding of current and emerging threats.

CPNI facilitates information exchanges which allow one company to learn from the experiences, mistakes and successes of another, without fear of exposing company sensitivities. Information exchanges are free to join and their membership is determined by the existing members.



Scenario 1:

Global telecoms firm loses out to competitor after cyber theft

What happened?

A sales director of a global telecoms company was targeted and had a corporate laptop stolen whilst attending an overseas conference. Given his position, he had access to key corporate information, including bid information for an upcoming major tender. A local copy of a database was stored unencrypted on the stolen laptop. The perpetrator retrieved this information easily and was able to pass it on to an unscrupulous competitor.

What was the impact?

The company lost the tender and market share to an overseas competitor and experienced a steady fall in share price. It was only after a lengthy internal investigation that the company became aware of the information breach, by which time it was too late.

How could this have been prevented?

For this scenario we suggest four of the ten steps are of particular relevance to mitigate the information risk:

Information Risk Management Regime
As a business heavily reliant on large industry contracts, the company should have recognised and valued its contract bid information assets and protected that data appropriately.

Removable Media Controls
Removable media controls would have ensured that data removed from the corporate network was appropriately protected, for example through encryption of the laptop.

Home & Mobile Working
A robust mobile working policy and an encrypted Virtual Private Network (VPN) would allow people to access the office network without the need for local copies of databases.

User Education & Awareness
The sales director should have been aware of the potential risks he might be exposed to and sought advice on how best to manage them.

Scenario 2:

Pharmaceutical IPR stolen in persistent cyber attack

What happened?

A world leading Biotech company developing the next generation of pharmaceuticals was ready for a product launch following five years of research and development representing a £1 billion investment. However, vulnerable systems and processes allowed it to become the victim of a sophisticated and targeted cyber attack allowing the attacker to steal the research.

Eight months before the product launch, the research director received an email that appeared to be from a colleague with a PDF of a relevant scientific paper. The email was actually a fake and the PDF attachment contained malware which exploited a software vulnerability for which the patch, although available for months, had not been applied. This well-fabricated social engineering attack allowed the attacker to steal the research and other sensitive information enabling a foreign competitor to release a cheaper version of the product onto the market ahead of the UK company.

What was the impact?

The company suffered material financial loss; they faced setbacks in securing further funding for research and development and lost major contracts to foreign competitors, who beat them to market with additional products based on the stolen research.

How could this have been prevented?

For this scenario we suggest five of the ten steps are of particular relevance to mitigate the information risk:

Information Risk Management Regime
The Board should have been aware of the value of their Intellectual Property and the cyber risks to the organisation of this type of attack. Appropriate security controls could then have been put in place.

Secure Configuration
Known vulnerabilities were exploited by this attack. All software should have been up-to-date and patched. A system lockdown could have prevented the attacker from installing their own malicious tools.

User Education & Awareness
Staff should have been trained and understood the importance of not clicking on links or opening suspicious documents in unsolicited email.

Monitoring
Active internal monitoring of valued assets, log analysis and web filtering all could have detected the attacker's activities.

Malware Protection
Software to detect malicious code could have prevented or limited the damage caused by the malware.

Scenario 3:

Security company crippled by politically motivated hacktivism

What happened?

A security firm with large Government contracts became the victim of a cyber attack by politically and ideologically motivated hacktivists.

A security flaw in a poorly designed public facing website enabled an attacker to gain access to an internal database which held passwords. A combination of weak passwords and poor password security management enabled the attacker to gain administrator privileges and as a result access to the company's entire IT estate. The attacker was then further able to exploit unpatched systems until they had access to the company's internal emails and sensitive data.

What was the impact?

After a number of sensitive internal emails and data were published publicly, there was severe reputational damage and a loss of customer confidence in the company. This led to problems with retaining both current contracts and securing new ones, ultimately leading to bankruptcy.

How could this have been prevented?

For this scenario we suggest five of the ten steps are of particular relevance to mitigate the information risk:

Managing User Privileges
Robust password management policies could have ensured strong and secure passwords, while user privilege management would have prevented abuse of administrator accounts.

Secure Configuration
Maintaining software reduces the risk from security flaws. Secure configuration of systems would have prevented the installation of malicious tools.

Information Risk Management Regime
The board was complacent in assuring that the IT department was implementing a compliance regime to required standards. A robust corporate governance regime would have spotted areas of concern before the attack.

Network Security
A segregated network would have limited the attacker's access regardless of the initial success of the compromise.

Incident Management
Incident management procedures would have alerted security to the intrusion and triggered procedures to mitigate the damage and limit future damage in the event of further attacks.

Managing Cyber Risks Within Corporate Governance

Like other corporate risks, cyber risks need to be managed proactively by the Board, led by senior management and assured by corporate governance. A model for managing cyber risks is suggested below. Implementation will clearly need to reflect the nature of your business and your appetite for risk.

Board

Make protecting your information a Board responsibility

- Have you agreed as a Board what information assets are critical to your business?
- Have you decided your appetite for risk with regard to these assets?
- Are you proactively managing these risks as a Board?

Cyber Risk Management - A Board Level Responsibility

Refine cyber stance

All Board Members

Request assurance

Regular information risk reports

Assurance findings

Business

Implement an information risk management regime

- Have you ensured that your existing risk management regime encompasses information and cyber risk?
- Have you implemented appropriate security policies & controls which you maintain?
- Do you maintain an up-to-date awareness of threats & vulnerabilities?

Typically CEO, CIO, CTO, CISO etc

Corporate governmance

Assure yourself that the information risk management regime is effective

- Have you assured yourself that you are managing the right information & cyber risks for your business?
- Are you implementing the right security controls at the right pace to meet your risk?
- Are you regularly testing, monitoring and reviewing your security controls?

Typically non-executive directors, chair of audit committee, risk committee.

Executive companion

Detailed guidance sheets

Cyber Security - the Next Steps

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

- Confirm that you have identified your key information assets and the impact on your business if they were to be compromised;
- Confirm that you have clearly identified the key threats to your information assets and set an appetite for the associated risks;
- 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; in the first instance audit partners should be able to provide assistance. For information risk management expertise, organisations should seek advice from members of appropriate professional bodies or those who have attained industry recognised qualifications.

There are a number of professional services schemes overseen by CESG (the Information Security arm of GCHQ). Whilst these are primarily aimed at the public sector, they may be of assistance to the private sector. To see the range of professional service schemes overseen by CESG to assure quality in people, products, services and systems visit **www.cesg.gov.uk**

Sources of further information

For any specific queries on the content of this booklet please email **cybersecurity@bis.gsi.gov.uk**

The Top 20 Critical Controls for Effective Cyber Defence provides additional information on a range of quick wins through advanced technical measures. See: **www.cpni.gov.uk/advice/cyber**

For further information on the CPNI information exchanges, see: **www.cpni.gov.uk/about/who-we-work-with/Information-exchanges**

To report fraud and internet crime contact Action Fraud at **www.actionfraud.police.uk** or call 0300 123 2040.