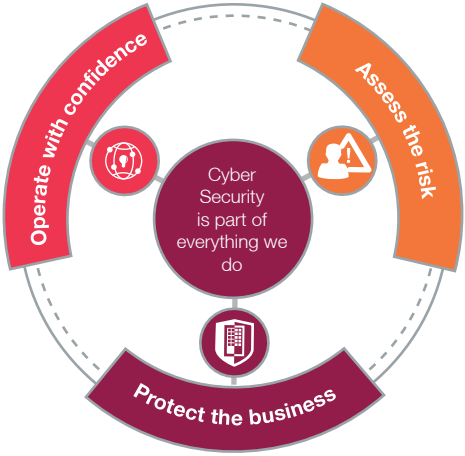
THIN **GUIDE**

Cyber Security for Business

A plain language guide presented by CGI

CGI

Experience the commitment®



At CGI, cyber security is part of everything we do. For more than 40 years, we have helped clients manage complex security challenges with a business focused approach – protecting what is most valuable to them.

For more information please visit www.cgi-group.co.uk/cyber or email cyber@cgi.com.

Foreword

As our companies and economies become digital in nature, securing our organisations against cyber attacks and data breaches has become one of the most important business issues facing senior management. Yet useful information about cyber security, especially for board level executives, is hard to find. It is a tough subject to understand, surrounding itself in jargon while undergoing seemingly constant change. It's also a difficult area to manage - when you're getting cyber security right, nothing happens; you only know when you've got it wrong.

Board-level decision-makers bear responsibility for ensuring their companies are protected from the reputational and financial damage that a cyber attack can inflict on their organisations, their customers, even their staff.

In plain and succinct language, this book explains some simple and practical measures that senior decision makers can take to improve their organisation's control over cyber security. I wholly support the aims of this, the first in the THIN **GUIDE** series, to provide essential management guidance on the complex topics of our day.

If you do nothing else, skim the headings and action lists in each chapter and think about how you apply the advice to your company. It might make all the difference.

Richard Holmes,
Head of Cyber Security Services, CGI UK.

CGI

THIN **GUIDE**

Cyber Security for Business

Published by Thin Guides Limited, London
Email: info@THINGUIDES.com

Typesetting and artwork by Global Design & Language Solutions Limited (GDSL), London.

Printed and bound by Mayfield Press (Oxford) Limited

The authors would like to thank Andrew Rogoyski for his invaluable contributions to this THIN **GUIDE**.

www.THINGUIDES.com
Registered in England and Wales. Company Number: 09094616

THIN **GUIDE**

Cyber Security for Business

Authors

David Topping
David Tebbutt

Glossary

BS 10010: An information classification, marking and handling standard

CiSP: Cyber Security Information Sharing Partnership set up to exchange cyber threat information

COSO: Committee of Sponsoring Organizations provides guidance on threat management

CSAT: A generic term for Customer Satisfaction ratings

DPA: UK Data Protection Act is 1998 legislation superseded by the Data Protection Bill (GDPR implementation)

DPO: Data Protection Officer – a board level appointee mandated by GDPR for many organisations

GDPR: General Data Protection Regulation (UK Data Protection Bill) protecting EU citizens' information

ISO 27001: Comprehensive information security management standards

IoT: Internet of Things – internet-connected objects that collect and exchange data

ISMS: Information Security Management System

Malware: Group category for any piece of software designed to do harm or cause loss, comes in many varieties such as Viruses, Trojans and Worms

NCSC: National Cyber Security Centre helps protect critical services, manage major incidents and provide technological improvement and advice

NISD: Network and Information Security Directive protects critical national infrastructure IT systems

PCI DSS: Payment Card Industry Data Security Standard

PECR: Privacy and Electronic Communications Regulations restrict processing and sharing of personal data on the internet

Phishing: A contact (email, text, phone) to get you to reveal personal details, click on a malicious link or transfer money

Contents

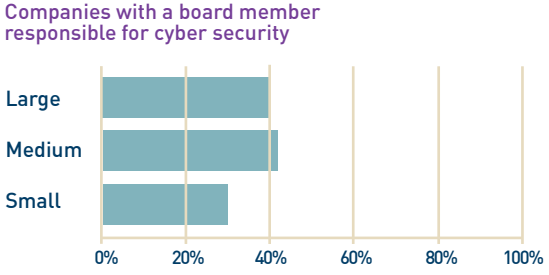
Establish leadership

Cyber security is a board level responsibility. Information technology is so prevalent it is hard to imagine how a company could work without it. In fact, most companies would cease operating without their information systems.

Even relatively minor 'cyber incidents' can lead to a loss of reputation or customer confidence and a subsequent loss of profit and shareholder value. Poor cyber security might cause you to experience such an issue. That's what makes it a board level problem.

Cyber security doesn't just happen; it's not something that the IT department can fix on its own. It has to be a company-wide and inclusive initiative and it has to be led from the top.

Yet, figures from a Department for Culture, Media & Sport (DCMS) survey by Ipsos MORI and the University of Portsmouth show that only a minority of UK companies have assigned responsibility for cyber security to a board member:



Appoint a cyber leader

One of your first actions should be to appoint someone to lead your cyber security efforts. They have four primary responsibilities: representation, management, compliance, and improvement.

Representation

The cyber leader's most important role is to create and spread awareness of cyber security and its requirements. This will involve evangelism and promotion as well as rigour and ability to deliver.

They need to represent cyber security interests at board level, to the company as a whole, and to external business partners. They also need a basic understanding of all stakeholders' interests, requirements and obligations. As such, they will need to be a good communicator, business savvy and a strong influencer.

Management

The cyber security leader has to manage the company's efforts across multiple departments and interest groups and create actual or matrix teams to assess risk and develop policy, respond to incidents, create and run awareness, education and training programmes.

In addition, this role carries responsibility for information assets, hardware security and even the security credentials of employees.

The leader needs to be the clearly identifiable single point of contact for cyber security issues, inside the company and for external partners and the public. They need to be suitably empowered and have the appropriate authority to make sure that things happen.

Compliance

Where the company is subject to regulation or standards, as most are, the cyber security leader needs to understand enough of the regulations to know how to comply and then monitor that compliance.

Compliance works beyond your own organisation – the cyber security leader needs to ensure that suppliers and partners are obliged to comply with your security rules, policies and standards.

Improvement

Threats, technology, regulations, partners and employees all change over time. They need to be monitored continuously and your cyber security needs to be measured, monitored, and improved to match those changes.

Incidents and simple accidents happen and, even after successfully managing them, the lessons learned have to be included into new programmes to prevent recurrence. Your leader needs to make sure this happens.

Who is your leader?

It might seem that the person needed for the role of cyber leader is a professor of computing, with a law degree and great communication skills.

The real requirements are not solely cyber skills, but 'sufficient knowledge', management ability, credibility, and personal authority. It is more important to have someone who can deliver effective cyber security than someone with the best security qualifications.

Although every company needs a cyber leader, not all companies are big enough or can afford to have a dedicated role. Smaller businesses can look at adding the responsibilities to an existing board member. Given that cyber security affects the whole business, the CEO needs to be fully supportive of whoever is chosen. In the event of a cyber security incident, the CEO's involvement and understanding are critical.

Having said this, even if your business is relatively small but technology is central to it, or if it is based on digital intellectual property, or it processes significant amounts of personal information, then a dedicated main board position may be advisable.

Cyber security can no longer be solely the responsibility of IT. Effective computer systems underpin the entire company's activities and can make the difference between success and failure. The board is responsible for good security. This means you need someone at the most senior level in your company who can effectively deliver it.

- Make cyber security a board level topic
- Appoint an effective management leader of cyber security with clear authority
- Ensure that the CEO is fully supportive of the role

Appoint a response team

"If something can go wrong it will go wrong". At some point, your company will face a cyber security problem. It could be malicious, accidental or simple failure of computer equipment. It will affect your business.

The first few hours of an incident can make a significant difference to the severity of the outcome. The priority is to assess the impact, fix the damage, deal with the cause and mediate any liability. Don't lose those hours by missing that an incident has taken place, by the wrong people trying to deal with it or, worst of all, ending up with a 'blamestorming' exercise while the problem remains.

Nominate a team of people now. Even if they don't yet know what their roles and responsibilities will be, their first job will be to find out.

The response team

The people on a response team will vary, the responsibilities don't. The essential roles needed are:

Main board member: Responsible for ultimately deciding on and authorising the recommended actions of the incident manager.

Incident manager: Responsible for assessing and overseeing a) the severity and initial response and b) the entirety of the actions undertaken to stop, mitigate and repair the incident.

For the sake of efficiency, other team members may temporarily report to the incident manager.

Communications manager: Responsible for communication with stakeholders including customers, the public and investors. Also responsible for internal communications to inform the rest of the company of the status of an incident.

Legal advisor: Responsible for presenting a clear view of obligations under legislation such as the General Data Protection Regulation (GDPR), the Network and Information Security Directive (NISD) and other legislation, regulations or contracts that apply to the company (or its IT suppliers or other business partners).

IT security specialist: Responsible for understanding a breach, reporting on how it occurred and recommending actions to prevent any similar future breaches.

Table exercise

The simplest and most effective way of getting a response team to work is a 'table exercise'. Participants role play an incident such as a data breach and respond with their current level of knowledge about incident management, the processes involved, the people involved, and so forth. This may be an area where the ISO 27031 standard or external cyber security guidance will help.

The table exercise is training; it will help the team understand and agree what the priorities must be, how to work with each other, how the CEO wants to hear recommendations, and how they might implement the decisions.

In addition, it identifies what skills or knowledge are missing. In this case, the answer "I don't know" is a good one, it clearly identifies that something is missing and provides an opportunity to fix things before a real incident happens.

The exercise also gives an idea of the time and management distraction an incident can cause, and why the remedy should be left to people who have practised it. Many companies will find that they need external expert help. They need to identify these resources before an incident occurs. It is a good idea to have experts on a retainer so they can invest time in understanding how your company works. At the very least, have them on speed dial.

The response team cannot be brought in on an ad hoc basis, without prior training. Ideally, they are a team that has run through distinct types of incidents and role-played what they will do; documenting the possible actions into a 'playbook' or decision-tree matrix that other people can use and understand in their absence.

- Appoint the response team
- Run simulations
- Identify lack of internal skills / knowledge
- Get the necessary skills and knowledge
- Appoint third parties to plug the gaps
- Document the priorities and processes for others
- Repeat the process

Understand the threat landscape

To assess your organisation's vulnerability to a cyber attack, ask yourself "What would motivate an attacker to get hold of our valuable information?"

Some might encrypt your files until you pay a ransom. Some might steal credit card data to sell to fraudsters, while others might steal proprietary information to sell to competitors. Idealists might deface your website because they object to your business activities. Hacker enthusiasts might simply want other hackers to know that they have the skills to penetrate an organisation. Insiders might do it out of ignorance, incompetence, or because they harbour a grudge.

Part of understanding the threat landscape is identifying what an attacker might hope to accomplish and what impact it would have on your organisation:

A ransom payment could be small compared to the disruption costs of non-payment, which is why affected organisations are often tempted to pay up. However, they have no guarantee that the perpetrator will restore their systems and it is worth noting that it is illegal to pay a ransom to any organisation that might have links to terrorism.

A competitor could benefit from learning details of your confidential contract bids or business plans. Extremely unscrupulous businesses might hire a hacker to acquire such material.

Idealists (or 'hacktivists') might deface your website, disrupt your services, do anything, in fact, to create a news 'hook' that promotes their point of view while embarrassing your company.

Hacker enthusiasts may simply want to be noticed for their technical prowess and often don't intend to damage an organisation's systems.They're most likely to target well known organisations.

The results of these activities, and others, could result in financial losses due to disrupted operations, a fall in share price and/or reputational harm. If the breach were bad enough and you couldn't show that you've made appropriate preparations, you might be fined by a regulator and ultimately a loss of confidence in the leadership of the company could result in dismissal.

Access

To conduct a cyber attack, a perpetrator needs to infiltrate your system using vulnerabilities that typically exist in any complex IT system. They can exploit these from the outside through known infrastructure, operating system and application vulnerabilities or from the inside through the unintentional or deliberate action of someone with access to your information systems. This could be a staffer, an ex-employee or any third party business partner who has a login. In some cases, the attackers might use social engineering to trick the employee into disclosing security credentials or initiating a fraudulent transaction.

The most likely unintentional ways for malicious code to enter your system would be to fool a logged-in user into clicking on a link to a website deliberately infected with malware, open an email attachment containing malware or even to get them to plug in an infected memory stick.

Once inside your perimeter, many kinds of malware are adept at hiding themselves inside or alongside other, legitimate, software.

A deliberate attack by a disgruntled insider is another matter; depending on their access privileges, they can cause serious harm by abusing their authority or by copying confidential material to the outside world. Bear in mind that acts of ignorance, negligence or stupidity can cause exactly the same problems, so it's important to make sure that only the right people have administrator privileges for your systems.

Figures from Ponemon Institute's 2017 *Cost of Data Breach* study show UK cyber breach sources:

Other research reveals a similar pattern, making it clear that training system users – whether staff or contractors – needs to be a major element of your 'protect and prevent' strategy.

Prioritise

Consider which types of attack are most likely to affect your organisation and, therefore, what kinds of defences are appropriate. You don't need to try to guess the details of every possible attack or who the perpetrators might be; you will have the right experts on board to go into this kind of detail. At a strategic level, you will at least be able to share your thoughts on likely attackers and have a reasonable

chance of understanding, and exploring your experts' insights to better understand your position.

First, prioritise the security of the information your company holds that is the most precious. This might include personal, sensitive, financial or strategic data. All subsequent protective measures will flow from this understanding. Then, when deciding on the appropriate measures to protect your organisation, consider factors such as the anticipated cost of a breach against the cost of preventing it and how much risk you're prepared to live with. Essentially, treat cyber security as a business risk like any other.

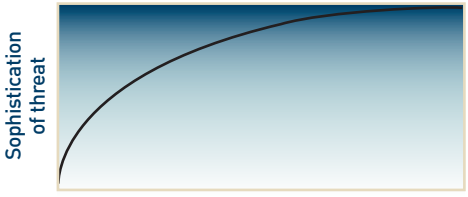
The insider threat

Anyone connecting to your system – and that might, but probably shouldn't, include third parties such as consultants, suppliers and customers – can potentially get within your security perimeter. All users need appropriate security guidance and a level of access that matches their level of authorisation and the systems/devices they use. Watch for unusual behaviours such as a user accessing files that they've never accessed before, large print jobs and other anomalies that can indicate an insider problem.

- Be clear about your adversaries' motivations to attack your business
- Identify the information that is most valuable to your business
- Have systems in place for detecting and dealing with breaches
- Have an awareness and training plan to protect against human error

Assess risk and scope

Cyber security risk is a normal business risk; your management and not just your IT department or advisors should assess it. Like any other risk, as management, you need to balance the costs of any action or inaction against the likelihood of gain, loss or damage. Most companies can secure themselves adequately at reasonable cost. However, if they are subject to significant risk, their costs will be disproportionately higher:



At some point, the law of diminishing returns becomes evident – you can never protect yourself against all attacks, it's a matter of balancing the likelihood, the impact, your appetite for risk and the investment you are willing to make to protect your organisation.

Broad risk assessment

Even before you go through a risk assessment process, you can ask some simple questions at board level to set the overall scope and approach you take to risk.

- Size and complexity?
- Nature of business?
- Profile and Reputation?

The number of employees you have, the number of subsidiaries or associated companies you have, the technology platforms you use, the market sector you operate within and the amount of business you have with third parties around the world will all factor in to how much risk and effort you face in implementing good cyber security. A small business that depends on the development of intellectual property, to provide confidential advice or that holds financial information is potentially a high cyber security risk. Household names and those with a global reputation are also attractive targets.

Assessing the broad issues above can help define an appropriate amount of effort you put into a risk assessment process.

Cyber risk management stages:

- **Discover your information and IT assets**
- **Assess the value to the company**
- **Assess the costs of protecting them**
- **Make and communicate your risk decisions**

Discover

First, you have to find out what you have, where and how it's held and by whom. This should start with discovering and then auditing the information and data your company deals with on an everyday basis. This means you must include information users, not just depend on IT or an external advisor.

Some items are obvious: databases, business applications for your accounts, customer relations and manufacturing processes, for example.

Everyday users will help you identify other, difficult to find, items referred to as 'unstructured data',

which includes management reports, spreadsheets, even presentations that contain business sensitive information that may be regularly exchanged or sent outside your business, or handled by unauthorised, unvetted, employees or contractors. It will also give you an insight into unexpected risks such as customer lists held on mobile phones, unreleased annual reports stored on public cloud servers, how prevalent the use of unauthorised cloud services is, or whether staff are leaving printed documents lying around unsecured.

Assess value

Every company is different but the value of IT systems and information can be judged on what happens if you fail to maintain confidentiality, the data's integrity or availability to the data. This 'CIA' approach is fundamental to understanding the value of a data asset. In the context of 'CIA', ask how much will it:

- **Cause harm or embarrassment to the organisation or individuals?**
- **Create a direct loss or loss of profit through disruption?**
- **Cost to repair lost or corrupted data?**
- **Make you subject to prosecution or fines?**

The answer will vary for each system or type of information. From this, you can develop a hierarchy of importance and an estimate of potential damage. Loss of a core business IT system can be catastrophic, but so could the loss of future profits from investment plans or a unique business process exposed to competitors. Breaches of regulations such as GDPR potentially carry very significant fines as well.

Assess costs

Having a comparison of the relative value of information and systems, as well as an overview of your threat landscape, allows you to prioritise your cost assessment on a management, not technological, basis. You may not be able to estimate the costs yourself but, if the greatest threat is loss of a core business application from hacking, it is worth asking IT to spend money to assess the cost of suitable protection. If the greatest risk and exposure is employees sending out highly sensitive information, then obtaining the cost of a data loss prevention system, or a change in internal processes, becomes a priority.

Make and communicate risk decisions

Exactly how you allocate budgets will be unique to your business, but identifying and securing your company's 'crown jewels' and its greatest exposures are key. Some of the simplest and least expensive actions can provide the most effective protection. For example, patching computers and devices, publishing and communicating a security policy that represents your risk decisions, providing staff awareness and ongoing training or using standards such as ISO 27001 for systems security and BS 10010 for information classification, marking and handling – these simple steps can improve your cyber security as much as the most complex software.

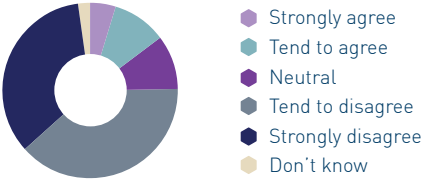
- Find out what you have and where it is
- Assess potential loss and how at risk you are
- Apply security controls where they are most needed
- Communicate your decisions to the company

Create a company-wide culture

Cyber security strategies that look at employees solely as a risk factor is poor cyber security. Good cyber security looks at them as the front line of defence. You simply cannot deliver good cyber security without the active, willing and informed involvement of the company and everyone within it.

You, your colleagues and your staff depend on IT to get their jobs done. Your business also depends on it but, in the battle between getting the work done 'on time' and getting the work done 'securely', 'on time' wins. Every time.

The emphasis on cyber security gets in the way of our organisation's business priorities:



Statistics from DCMS *Cyber Breaches Survey 2017* by Ipsos MORI and University of Portsmouth

This can lead to a conflict between those planning cyber security and those having to use it. It's visible in everything from the use of quick and easy but non-secure cloud file sharing for business-critical documents, to the refusal to adopt an unwieldy password policy.

You can't just hope for 'buy-in'; you need to include the whole company in cyber security from the start so that everyone sees it as part of the company culture and accepts it because it makes sense. Not 'their' but 'our' cyber security policy.

Inclusive security

Your cyber security could fail at the first hurdle if it's designed solely by your IT department. IT is responsible for security technology but not for the wider aspects of information security.

Create a team from different departments across the company, with IT department or external guidance that can:

- **Provide a practical audit of your information and the devices they use**
- **Assess the value of different types of information**
- **Set realistic requirements for everyday controls such as system access and password policies**
- **Look at how to alter departmental processes to provide protection against threats such as 'CEO fraud'***

An added advantage of such inclusion is that external skills can be transferred into the company and made relevant to different departments. It will also create a team of knowledgeable inside evangelists who can further help with awareness, education and training.

** Staff member tricked by a fake CEO communication into transferring money to a fraudulent bank account.*

Awareness, education and training

Awareness, education and training are vital in creating cultural shifts within an organisation. But they are not the same thing. They perform equally important functions and should be co-ordinated to work together.

Awareness

Management is responsible for creating company-wide awareness of the importance of cyber security and its consequences. Messages about the importance of cyber security have to be seen to come from the top of the company and to be as important as any other strategic initiative.

This is a communications campaign aimed inside the company; perhaps run by people from the communications department if you have such specialisms. The aim is to promote the importance of cyber security and to steer people towards getting education and training and then applying it to everyday situations.

Marketing departments have come up with ideas to promote cyber security awareness, including tradeshow stands in foyers, viral advertisements, posters, internal mailings and even promotional items and competitions. Simply put; use the best resources you have internally to raise awareness – it's a worthwhile investment.

Education and training

Education explains the principles of cyber security, some of the threats and traps, and the company's policy. Training gives your people the necessary skills. Both are equally important but might be provided to different groups. Education may be more appropriate to those who deal with more sensitive information or systems. They are the people who need to know the reasons for an information security policy in order to extrapolate from it to deal with unforeseen situations. Training should aim to get the whole company to adopt a standard set of behaviours.

Education and training are both part of personnel development and an HR department can treat this as a (possibly mandatory) additional staff development course, developing it with IT and the team that developed policies and controls. In the absence of HR or IT with sufficient skills, many off-the-shelf courses are available from cyber consultants, although they should be selected on the basis that they align to your company's strategies and policies.

Company-wide

Company-wide has to mean everyone. Cyber security initiatives can fail if the most senior managers don't take part. That means being seen to support the development process, supporting the awareness, taking part (visibly) in the education and training and, ultimately, following the policies.

Continual improvement

Awareness, education and training have to be ongoing. Threats vary and develop, your IT systems and defences will change and your policies will change to match them. These changes need to be communicated.

You need to measure improvements. This could start with the number of people being trained. Some companies develop online tests to create an ongoing score for cyber security familiarity, others use the IT department to measure user-based incidents, and some even get staff competing to write good phishing emails.

- Involve people from across the company in cyber security development
- Develop and deliver awareness, education, and training as separate items
- Constantly assess, review and revise

Keep on top of legal landscape

It is important when choosing your business partners, or they when choosing theirs, that their approach to cyber security represents best practice for the type of company they are. A quick way is to check this through their certification. A good prospect would have ISO 27001 certification. Government-backed schemes such as *Cyber Essentials* and *Cyber Essentials Plus* offer an indication of good practice. *Cyber Essentials* is now a minimum standard for all Ministry of Defence suppliers with contracts that involve sensitive or personal information.

However, any company that tries to base its security strategy purely on regulatory obligations will fail. It is important that you go beyond these regulations and frame your security around your company's entire commercial and governance needs. And increasingly, laws such as GDPR (see below) are not compliance regimes, so there is no right answer or guaranteed set of steps that a company needs to make to be prepared – it comes down to demonstrating sound judgement on the topic.

The computer security world is subject to many laws, some of them such as the Computer Misuse Act date back to the 1990s. In terms of standards, they are many and various – it requires a mixture of judgement and expertise to decide which are appropriate for use in your company. A report, *UK Cyber Security Standards*, published in 2013 by PwC for the Department for Business, Innovation and Skills (BIS), identified 128 standards and guides relevant to cyber security. Your legal experts, security professionals

and management should all be familiar with the important laws, standards and codes of practice that govern your own company's needs. If in doubt, get some advice.

Legislation

A few of the most important pieces of legislation that are relevant to cyber security are listed below.

GDPR (General Data Protection Regulation)

GDPR is one of the most significant pieces of legislation affecting privacy, data protection and cyber security. It supersedes the UK Data Protection Act (DPA) 1998. GDPR is aimed at protecting the digital rights and privacy of all EU citizens. Its implications affect every business that deals with the 'personally identifiable information'. The regulations are complex but what every senior manager should know, at a minimum, is that GDPR:

Requires an organisation to have a lawful basis for processing personal information, or informed consent from the data subject

Applies if your company (or any of your service providers) holds any personally identifiable information about EU citizens

Carries substantial fines for non-compliance – up to €20m or 4% of global turnover (whichever is greater)

Has almost no exemptions – it covers 'any legal entity engaged in economic activity'

Requires companies that carry out certain types of processing activities, and all public authorities, to appoint a Data Protection Officer (DPO)

The DPO must be independent, knowledgeable about data protection, have adequate resources, and report to the highest management level

Requires notification of breaches within 72 hours to authorities, and to data subjects if the breach adversely affects individuals' rights and freedoms

Enshrines a number of rights for citizens such as the right to understand what data is held about them, the right to correct it and, if appropriate, the right to erase it

Requires adoption of a set of principles that include 'designing in' privacy and security at all levels within the business, from strategic planning to everyday operations

Some government bodies see the GDPR not only as a means for companies to protect personal information but also as a catalyst for wider cyber security awareness and action.

However, if you have implemented a good data protection and cyber security policy, you may find that you are already prepared for GDPR. If you haven't, then the actions you have to take to comply with it will be a significant step towards an effective overall cyber security policy.

NISD (Network and Information Security Directive)

NISD is another EU initiative, affecting companies working on essential infrastructure such as banking, energy, transport, health, water and digital service providers operating in the EU. It requires public disclosure of breaches and its fine levels are in line with the GDPR's.

PSD2 (Payment Services Directive 2)

PSD2 is aimed at payment service providers (PSPs), including banks. Organisations must report security incidents to regulators. Customers must also be notified if an incident could affect their financial interests.

PECR (Privacy and Electronic Communications Regulations)

PECR is an established piece of legislation that affects organisations that indulge in or facilitate direct marketing communications and those who use cookies or similar technologies to track visitors to their websites. It is still evolving and is likely to be superseded by a new e-Privacy directive from the EU.

Computer Misuse Act 1990

The Computer Misuse Act is intended to deter people from using a computer to assist in the commission of a criminal offence or from interfering with the ability to access data stored in an IT system. The Act contains three criminal offences: unauthorised access to computer material, access with intent to commit further offences and modification of computer material.

These laws, and more, are complex. If in doubt, seek expert advice.

Standards

Hundreds of standards apply to cyber security, ranging from management frameworks to the specifics of a piece of technology. If you are obliged to use any cyber security standards and you are unfamiliar with them, it is well worth obtaining specialist advice.

ISO 27000-series

This offers a rigorous and comprehensive family of standards for protecting and preserving your information under the principles of confidentiality, integrity and availability. It is the most important ISO document when it comes to cyber security.

If you start with ISO 27001, adapting to the requirements of the other standards should be a relatively smooth process.

ISO 27031, 27032, 27035

These standards are management-focused cyber security guides. They cover respectively: improving ICT readiness to ensure business continuity in the event of an uncontrolled incident, improving cyber security and linking it to other forms of security, and rapidly managing incidents.

BS 10010: 2017 (Information Classification, Marking and Handling)

British Standard 10010 provides a pragmatic methodology for securely managing information in any form: text, pictures, audio recordings, and not just 'structured data'. It also helps companies to exchange information securely with other companies and third parties.

Remember: cyber-aware suppliers and customers will be checking your security credentials too.

- Know why regulations, codes of practice and standards are merely a starting point for an effective cyber security strategy
- Make sure your security professionals are familiar with their requirements, e.g. GDPR and ISO 27001
- Make sure they are aware of other legislation, standards and obligations specific to your company and your industry
- Make sure all your third party contracts include a requirement for compliance with relevant standards

Know your partners and suppliers

For a cyber security strategy to be effective, it has to include any person, organisation or object that exchanges data with your IT system. Each poses a possible entry point for a cyber attack.

Because each of your business partners or suppliers faces similar risks, you need to ensure that their security measures match your own needs. This applies to existing relationships as well as new ones.

Your cyber security team needs to assess each of these stakeholders, explain your security requirements to them, contractually agree responsibilities (on both sides) and ensure their system access is appropriate to their function.

Statistics from DCMS *Cyber Breaches Survey 2017* by Ipsos MORI and University of Portsmouth

Assess stakeholders

Cyber security stakeholders include everyone who interacts with your IT systems. Some, such as visitors to your website who provide personal information in exchange for a report download, for instance, may not carry responsibility but you still bear responsibility towards them. Putting them to one side, the remainder

are those who, to any degree, are able to exchange data with your system. They include all staff with access devices – laptops, mobile phones, PCs, tablets, and so on. They also include some or all of your external suppliers and customers, including IT and other service and product providers. No-one, not even long-term providers, should be exempt from your scrutiny.

You will need to determine the level of access they have, whether it is appropriate and, according to that assessment, find out whether their security regime is sufficiently robust to protect you. In other words, you need to know who you can trust. Check their certification such as ISO 27001 or Cyber Essentials and include a check on the certifying authority. They are not all equal.

You also need to cover the security of devices attached to your system, locally or remotely. These could range from mobile phones, to handheld warehouse terminals, to security cameras. Each provides a potential entry point for a cyber attack. The advent of the Internet of Things (IoT) – home monitoring, smart meters, and motor vehicles, to name but a few – massively increases the 'attack surface' (the number of ways in which an attacker could get in).

Security requirements

Before you can embark on any security discussion with your stakeholders, you need to be unambiguously clear about your own requirements. You will then need to extract just the relevant requirements for each type of stakeholder. While an IT service provider might be happy to work with your full requirements, a small or medium business that interacts only with the purchasing department will need far less.

You will need to take a view on what you mandate for all your suppliers (and customers) and what you're prepared to slim down for special cases.

Responsibilities

The responsibility of maintaining good cyber security lies with all parts of your business ecosystem. You expect your stakeholders to be sufficiently secure and they expect you to support their efforts. You will provide updates to requirements and new discoveries that affect them and you will expect them to reciprocate with reports of relevant cyber incidents and actions taken. Ideally, you need to include your cyber security expectations in your commercial contracts. These will include aspects such as what to do in the event of a data breach or what should be done with shared data during the execution of a contract or at its termination.

System access

From a new joiner to a long-term IT service provider, the level of access to your system needs to be controlled. Always work on the principal of 'least privilege' – if a third party needs access to your applications and data, you should start by challenging whether it is really necessary and, if so, then ensure that they have only limited and appropriate privileges.

Were all these steps to be covered conscientiously, you would be able to conduct business more confidently in a spirit of partnership with the stakeholders who would then be part of your extended cyber security regime.

- Assess all relevant stakeholders
- Know which ones to trust
- Agree requirements and responsibilities
- Control system access

Know how to get good advice

Unless you are exceedingly fortunate, you will find that your internal cyber security expertise doesn't completely cover your requirements. You will have to find one or more external sources of help. It is vital that the people and organisations you choose will be valued and accepted as an integral part of your cyber team.

To stand the greatest chance of finding such help, you need to be clear about your requirements and know how to assess the prospective consultancies. You will also need to check they deliver on expectations.

Identify your gaps

Once your cyber security team has determined your needs, it will have identified the relevant skills and experience from inside the company. It will then have to draw on external services to compensate for any gaps. Given the breadth of cyber security, few consultants or consultancies can cover all the ground. To avoid overlaps and unnecessary complexity, it is important to be very clear about what you want to achieve through third parties. Only then are you ready to go searching.

Find help

Thousands of cyber security specialists would probably claim to be exactly what you need. It might help to hire someone with appropriate expertise to help you identify likely prospects. The National Cyber Security Centre (NCSC), part of GCHQ, is a rich source of helpful information including a cyber security information sharing partnership (CiSP) and a list of

certified consultants with their accreditations and their specialisations. www.ncsc.gov.uk/index/professional-service

Look for expertise in:

- Creating security policies and strategies
- Risk management
- Assurance on effective security implementation
- Designing secure IT systems
- Incident response to help you through a data breach
- Legal obligations under laws such as GDPR
- Crisis management to help you respond to an incident
- Media handling to help you protect your company's reputation in a crisis
- Testing whether your systems can be penetrated
- Education and training which specialises in cyber security
- And many more...

Assess prospects

Shortlist prospective consultancies according to a number of criteria:

Relevance: Do they understand your industry and your niche within it?

Experience: How much relevant practical experience of your type of need do they have?

Staffing: How qualified and experienced are the staff they will deploy?

Certifications: Have they earned relevant certifications?

Independence: Are they vendor-independent?

Reputation: Find evidence of customer satisfaction from independent reviews, CSAT ratings, industry reputation and published works.

Your desk research will lead to a shortlist. Then you will need to ask them face-to-face to fill in any gaps. Their behaviour at this stage will tell you whether they are sufficiently open-minded and collaborative to work with you in a spirit of partnership.

Implementation

Having selected the right partner(s) from your shortlist, they need to become part of your team as quickly as possible. This means creating and agreeing plans, expectations and performance measures so that you can periodically measure the value they're delivering. The details are up to your cyber security leader, but they should include behavioural as well as technical measures. You need to know whether they're delivering the promised value and you also need to know if they are genuinely working as part of your cyber team. Remember that an important by-product for your company is the knowledge transfer that is bound to take place in a collaborative relationship.

- Determine what needs you cannot satisfy internally
- Specify exactly what you need from third parties
- Shortlist those that pass your assessment criteria
- Ensure they integrate with the teams and leadership
- Monitor their performance

Document everything

No one wants yet another set of documentation. However, documenting cyber security properly is the best way to plan, implement and manage it, as well as demonstrate compliance or good practice, just as you would for any other business critical function. It's also an important part of demonstrating your competence to regulators in the event of a breach, under law such as GDPR.

Your documentation should be designed to help and protect your business. It needn't be onerous, and it should be developed to suit the size and complexity of your business. It should also be pragmatic and affordable and, above all, it should be easy to read and understand.

The five broad types of documentation are:

- **Planning**
- **Training**
- **Reporting**
- **Evidentiary**
- **Contractual / legal**

Planning

Documents used for planning cyber security should cover the company's assessment of the types of information and data it holds, the value of that information and the assessment of risks or liabilities from losing it. It needs to include the physical infrastructure of IT and the actual location of the information, as well as understanding who has access to information and rights over it. Decisions about

policy, training, execution and reporting need to be produced in a form the whole company can understand.

Training

To implement cyber security, your employees need to be involved and trained. Doing so effectively means more than just a single training exercise. Publishing a plan for training allows them to see what's going to happen and get involved. Significantly improve cyber security by developing materials that are easy to read and understand. They should contain not just instructions but reasons for those instructions.

Reporting

It's important to know if the cyber security plan is being implemented and if goals are being met, but the company shouldn't be swamped with information it can't use. Design reports to include key measures against management goals that make sense as they cascade up the management chain to the board.

Evidentiary

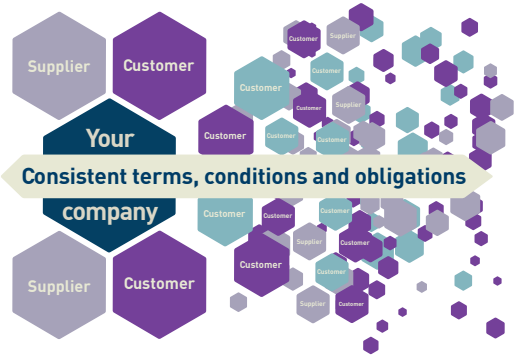
"If it isn't documented it didn't happen." Whatever 'it' is – a certification, a training schedule, a published policy, or an incident – if there isn't a record of it, you, as management, can't show what happened. If you face liability under regulations, the documentation of the efforts you made and your ongoing commitment to manage and improve cyber security can significantly mitigate your losses. Ideally, having clear documentation helps you avoid them altogether.

Contractual/legal

It's important when agreeing your contractual obligations to your customer to consider the security

obligations on your organisation, under law and by agreement.

This is a two-way process, so you should make clear the obligations that you wish to place upon your customer, such as appropriate use of IT systems you may be granting them access to. Bear in mind that your customer may not be the end-customer, so proper flow-down of terms and conditions that apply to areas such as data protection, breach response and other cyber security items, becomes very important.



What documents are required?

The documents your company needs to have or to produce will vary. Management needs only a set of documentation on which it can act. For any size of company, that set should include at least the following:

Information/data/systems audit

What information and data you have, where it is, how valuable it is and who has access to it and the systems it's held on. Assessment of third party IT supplier contracts and liabilities if they hold data for you.

Information/cyber security policy

Definition of valuable or sensitive information and data. Handling rules, where it may be kept, who is allowed access to it and the systems or devices it's held on and how they should be protected. A common type of policy is an information security management system (ISMS) which consists of a set of policies and procedures for systematically managing an organisation's sensitive data.

Cyber security plan

The company's current status, goals to meet the policy, training plan, reviews and progress made.

Cyber security report

System security status, any abnormalities, changes to structure or staff, incidents (which need to be notified anyway), outputs from automated monitoring (if installed) and other forms of monitoring.

Incident plan and report

A published plan for handling incidents developed by a response team and a formal report template for such incidents.

Cyber security board report and minutes

The synopsis of efforts to meet the plan, shortfalls and goals achieved. Must also include the minuted responses from the board. A common instance of this is a Security Working Group that convenes stakeholders from your organisation and your customers to agree progress, actions and other items.

Your documentation should be detailed enough to reflect your organisation's structure and complexity. For example, implementing the ISO 27001 standard will result in up to 17 planning and policy documents, nine mandatory reports and up to 16 others. They will more than satisfy the requirements above but many of them will be deeply technical and not relevant for management use without adaptation.

Several organisations have published useful generic cyber security management frameworks. Two examples are COSO's *Enterprise Risk Management* and Cisco's *Cyber Security Management Framework*.

Having documentation that suits your company, and your needs as management, is important enough that you should consider getting expert assistance to design it to suit your unique requirements.

Finally, once you've developed and documented your policies, plans, training schedules and reports, where will you keep them? Hopefully, securely backed up, offsite, and readily accessible in case of an incident!

- **Create a legible practical cyber security policy**
- **Create a plan that can be measured**
- **Create materials that educate and train staff**
- **Report on how the plan is being implemented at every board meeting**
- **Document all activities**

Create a review process

By now, your cyber security plan should be robust enough to deal with most types of everyday attacks, breakdowns and user errors. The details will change over time as the threats against your information assets change and as you find better ways to increase your protection. Cyber security risk reviews will become a permanent agenda item of board meetings.

Your cyber security framework determines all the primary areas of board level attention and direction – the 'why?' of the security strategy. They also address the 'what?' – the elements for which managers and digitally connected business partners will be responsible. Finally, at the 'how?' level, operational details will be defined. The framework itself will endure with little or no change because it was forged from a strategic, rather than an operational, perspective.

Your original goals and decisions will spread down towards everyone in the organisation. Each person will be responsible for minimising risk in their area of activity. Reports will flow back up, triggering local actions and summary reports that form part of the board's monthly discussions of new risks, the effectiveness of existing remedies and the bottom-line impacts.

At a strategic level, cyber security management is similar to any other major business activity. Perhaps the main difference is that cyber risk intelligence from the outside world, such as the NCSC's CiSP, is of vital importance to your security planning.

Your plan

Tackling cyber security cannot be a one-off exercise. Prioritise the rollout of your actions according to the risks being tackled. Work on short, medium and long term (1-, 3- and 5- year) plans, make sure they harmonise with existing security activities and plans. Each action will have a meaningful measure so that its progress or completion can be reported coherently.

A 'framework' approach – where the whys, whats and hows are clearly identified – gives everyone involved the chance to understand and participate in the plan's creation. By being involved, the participants acquire a sense of ownership and commitment to making their parts work.

At all times, progress will be clear and remaining gaps identifiable by matching progress to the framework.

Review

Revisiting your plans to test your original assumptions, measuring progress towards your goals, ensuring that budgets are being used wisely and that you have the necessary resources are just some of the reasons why it is so essential to conduct reviews. Material for review should be relevant to its audience. While the board might review summary feedback monthly, others inside and outside the organisation will be reporting on their security activities as required by the plan, sometimes on an hourly or daily basis.

Some companies will employ internal audit teams to independently monitor the effectiveness of the security strategy. Given that your main thrust is to empower everyone involved, any such audit should be seen by all as 'checking that the plans are working'.

Who drives the plan?

The main driving force will always be the company leadership team, which will include your chosen cyber leader. However, everyone who is digitally connected to your network must be asked to conform to the obligations the cyber security plan places upon them.

Operationally, it is clear that some people are better at looking at things objectively and communicating their findings clearly. These rare individuals need to be identified and offered the extra responsibility. They would be providing a valuable service to both their colleagues and their managers.

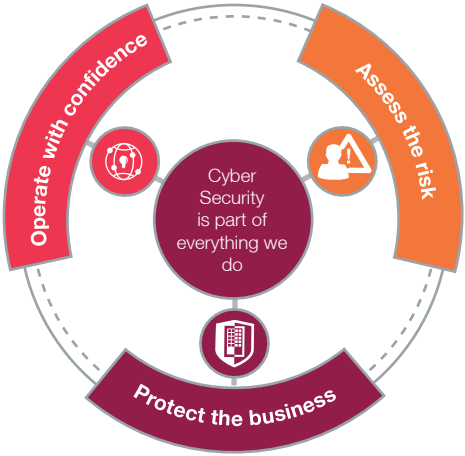
Why get involved?

Every person involved in the company's cyber security efforts will want to know "Why should I bother?" and "What's in it for me?" The simple answer is that their cumulative efforts will help their employer to survive and thrive, to maintain the organisation's reputation and to ensure that stakeholder data, especially that belonging to your customers, is safe and secure. Your cyber plan will ensure that everyone knows exactly what is expected of them.

- This is a business process, plan accordingly
- Make your plans visible - involve everyone who impacts your cyber risk, inside and outside the organisation
- Ensure you have built in a bottom-to-top reviewing and reporting mechanism
- Motivate people to participate

CGI

Experience the commitment®



At CGI, cyber security is part of everything we do. For more than 40 years, we have helped clients manage complex security challenges with a business focused approach – protecting what is most valuable to them.

For more information please visit www.cgi-group.co.uk/cyber or email cyber@cgi.com.

THIN **GUIDE**

supported by:

techUK