National Cyber Security Centre
a part of GCHQ

Cyber Security Toolkit for Boards

Helping board members to get to grips with cyber security

Contents

Introduction

The vast majority of organisations in the UK rely on digital technology to function.

Good cyber security protects that ability to function, and ensures organisations can exploit the opportunities that technology brings. Cyber security is therefore central to an organisation's health and resilience, and this places it firmly within the responsibility of the Board.

New regulations (such as GDPR) as well as high profile media coverage on the impact of cyber incidents, have raised the expectations of partners, shareholders, customers and the wider public. Quite simply, organisations - and Board members especially - have to get to grips with cyber security.

Why have the NCSC produced a Cyber Security Toolkit for Boards?

Boards are pivotal in improving the cyber security of their organisations. **The Cyber Security Toolkit for Boards has been created to encourage essential discussions about cyber security to take place between the Board and their technical experts**.

What can this toolkit do for you?

Board members don't need to be technical experts, but they need to know enough about cyber security to be able to have a fluent conversation with their experts, and understand the right questions to ask.

The Cyber Security Toolkit or Boards therefore provides:

1. A general introduction to cyber security.
2. Separate sections, each dealing with an important aspect of cyber security. For each aspect, we will:
    - explain what it is, and why it's important
    - recommend what individual Board members should be doing
    - recommend what the Board should be ensuring your organisation is doing
    - provide questions and answers which you can use to start crucial discussions with your cyber security experts
3. Appendices summarising the legal and regulatory aspects of cyber security.

Getting started

Don't feel obliged to read the Cyber Security Toolkit in a single sitting. Think of it less of a manual to be read cover-to-cover, but more of a resource to be used to help you develop your own cyber security board strategy; one that can adapt to fit your own unique cultures and business priorities.

If you're not sure where to begin, we suggest you start with the Introduction to Cyber Security for Board members and Embedding cyber security into your structure and objectives.

About the Cyber Security Toolkit

The Cyber Security Toolkit is relevant for anyone who is accountable for an organisation in any sector. That could be a Board of Directors, a Board of Governors or a Board of Trustees. Additionally, technical staff and security practitioners may find it a useful summary of NCSC guidance, and can use the questions within the toolkit to frame discussions with the Board.

Cyber Security Toolkit: scope and structure

Good cyber security is all about managing risks. The process for improving and governing cyber security will be similar to the process you use for other organisational risks. It is a continuous, iterative process and comprises three overlapping components, summarised below:

1. Get the information you need to make well informed decisions on the risks you face.
2. Use this information to understand and prioritise your risks.
3. Take steps to manage those risks.

Crucially in order for these steps to be effective, you need to get the environment right, so we've included three sections that explain how to do this. The full structure of the Cyber Security Toolkit is summarised in the table below - click on a link to jump to the relevant section.

<table>
<tr><th colspan="3">Getting the environment right

Embedding cyber security in your organisation
Growing cyber security expertise
Developing a positive cyber security culture</th></tr>
<tr><td>1. Get the information you need to make well informed decisions on the risks you face.

Establishing your baseline and identifying what you care about most

Understanding the cyber security threat</td><td>2. Use this information to evaluate and prioritise your risks.

Risk management for cyber security</td><td>3. Take steps to manage those risks.

Implementing effective cyber security measures

Collaborating with suppliers and partners

Planning your response to cyber incidents</td></tr>
</table>

Note: You will be familiar with this type of process, and may have your own approach to managing risk within your organisation. The Cyber Security Toolkit therefore focuses on the aspects of the process that are unique to cyber security and need additional consideration.

How to use the Cyber Security Toolkit

The NCSC is often asked 'what does good look like?' The simple answer is 'whatever protects the things you care about'. This means that, whilst there is some good practice that applies in most situations, 'good' cyber security for one organisation may not be 'good' for another. 'Good' cyber security has to work for you; it has to be appropriate to your systems, your processes, your staff, your culture and, critically, has to be appropriate for the level of risk you are willing to accept.

Each section within the toolkit addresses three questions:

1. **What should the Board do?**

   This provides specific actions for the Board.

2. **What should your organisation do?**

   This provides information on aspects that Boards should have oversight of but are unlikely to be actively taking action on (though this is dependent on your organisational structure).

3. **What does good look like?**

   This provides questions (and potential answers) designed to generate discussions with your experts that can help the Board identify what constitutes 'good' cyber security within your organisation. The questions are only the start of the story; you may find that simply getting the right people in the room, engaged in meaningful discussions, can throw a light on what works (and doesn't work) within your organisation.

How we built the Cyber Security Toolkit

This toolkit was created by:

- listening to what Boards have told us they want to know
- applying the NCSC's unique insights into cyber security, and how attacks happen

How you can help

We want to keep adding to this toolkit as you encounter new cyber security challenges, so we'll need your practical experiences of the challenges and opportunities you encounter. Please let us know how this toolkit could be improved, what you liked (or didn't like), and suggestions for what could be added next. You can use the contact us form or email us directly at enquiries@ncsc.gov.uk .

Introduction to cyber security for Board members

What is cyber security?

Cyber Security is the protection of devices, services and networks - and the information on them - from theft or damage via electronic means.

What do I need to know about cyber security?

There are three common myths concerning cyber security. Understanding why they're incorrect will help you understand some key aspects of cyber security.

Myth #1: Cyber is complex, I won't understand it.

Reality: You don't need to be a technical expert to make an informed cyber security decision.

We all make security decisions every day (whether to put the alarm on, for example) without necessarily knowing how the alarm works. Boards regularly make financial or risk decisions without needing to know the details of every account or invoice. The Board should rely on its cyber security experts to provide insight, so that the Board can make informed decisions about cyber security.

Myth #2: Cyber attacks are sophisticated, I can't do anything to stop them.

Reality: Taking a methodical approach to cyber security and enacting relatively small changes can greatly reduce the risk to your organisation.

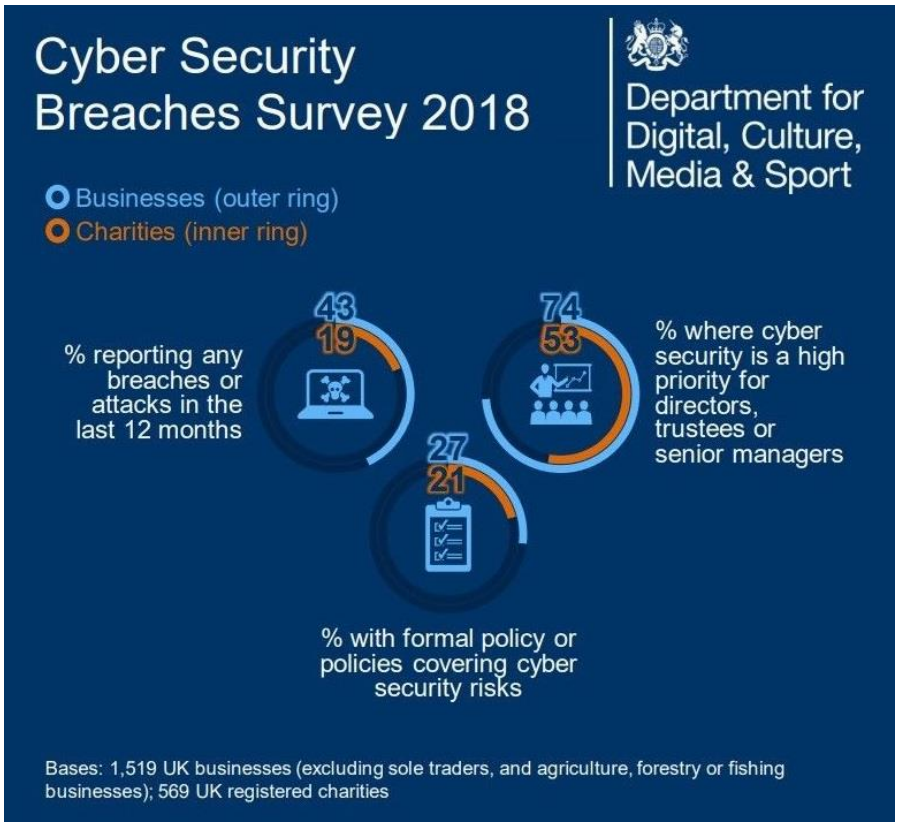
The vast majority of attacks are still based upon well known techniques (such as phishing emails) which can be defended against. Some threats can be very sophisticated, using advanced methods to break into extremely well defended networks, but we normally only see that level of commitment and expertise in attacks by nation states. Most organisations are unlikely to be a target for a sustained effort of this type, and even those that are will find that even the most sophisticated attacker will start with the simplest and cheapest option, so as not to expose their advanced methods.

Myth #3: Cyber attacks are targeted, I'm not at risk.

Reality: Many cyber attacks are opportunistic and any organisation could be impacted by these untargeted attacks.

The majority of cyber attacks are untargeted and opportunistic in nature, with the attacker hoping to take advantage of a weakness (or vulnerability) in a system, without any regard for who that system belongs to. These can be just as damaging as targeted attacks; the impact of WannaCry on global organisations - from shipping to the NHS - being a good example. If you're connected to the internet then you are exposed to this risk. This trend of untargeted attacks is unlikely to change because every organisation - including yours - will have value to an attacker, even if that is simply the money you might pay in a ransomware attack.

The findings from the Cyber Security Breaches Survey below show just how many organisations are coming under cyber attack and how organisations are responding to this risk. Further information is provided in the full report.



How do cyber attacks work?

A good way to increase your understanding of cyber security is to review examples of how cyber attacks work, and what actions organisations take to mitigate them. Reviewing incidents that have occurred within your organisation is a good place to start.

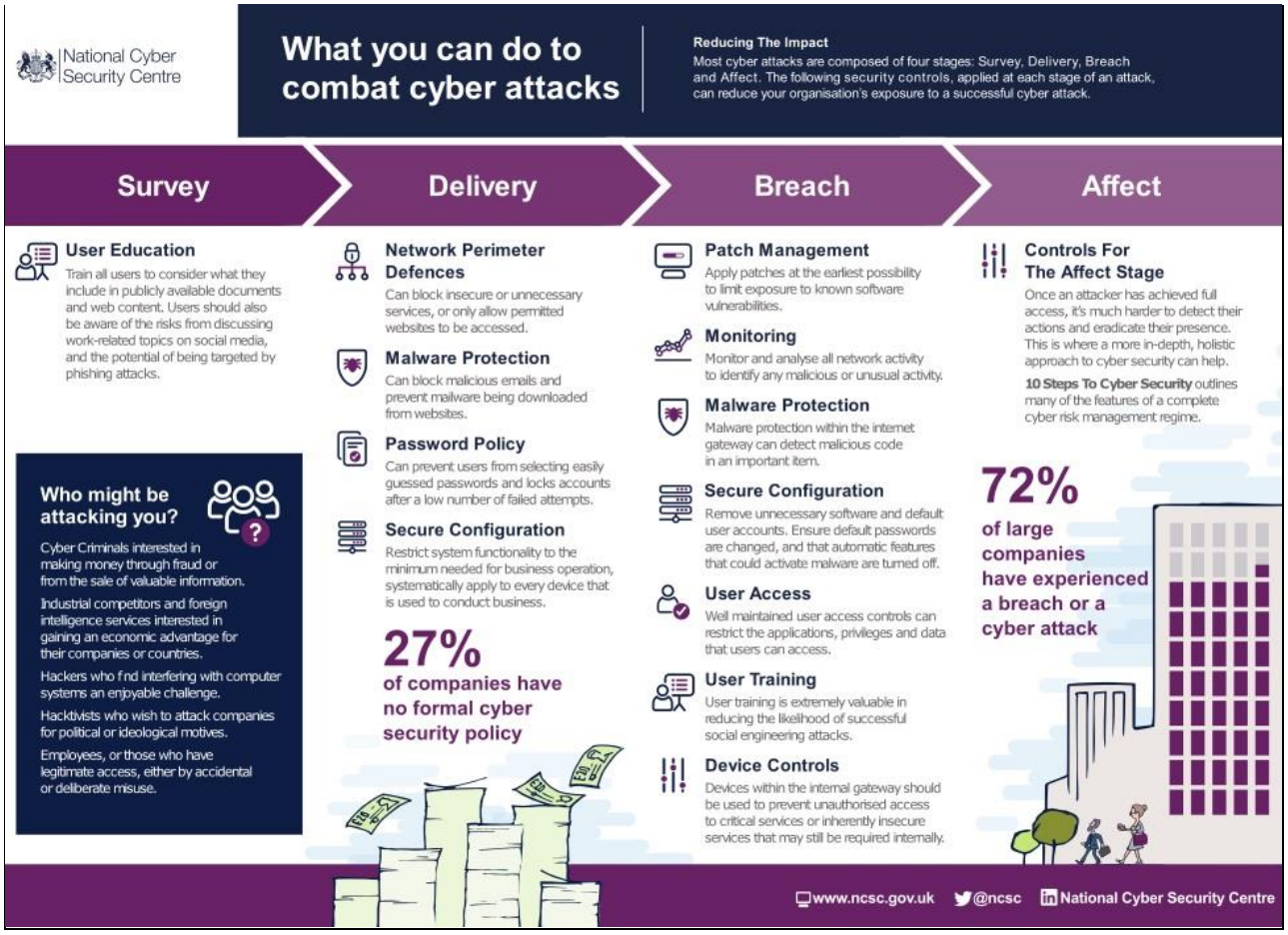
In general, cyber attacks have 4 stages:

- **Survey** - investigating and analysing available information about the target in order to identify potential vulnerabilities.
- **Delivery** - getting to the point in a system where you have an initial foothold in the system.
- **Breach** - exploiting the vulnerability/vulnerabilities to gain some form of unauthorised access.
- **Affect** - carrying out activities within a system that achieve the attacker's goal.

Defending against cyber attacks

The key thing to understand about cyber security defences is that they need to be layered and include a range of measures, from technology solutions to user education to effective policies. The infographic below gives examples of defences that will help your organisation to combat common cyber attacks. Our section on Implementing effective cyber security measures provides further detail and questions that you can use to understand more about your own organisation's defences.

The following infographic summarises the security controls you can apply to reduce your organisation's exposure to a successful cyber attack.



As a Board member, you will be targeted

Senior executives or stakeholders in organisations are often the target of cyber attack, because of their access to valuable assets (usually money and information) and also their influence within the organisation.

Attackers may try and directly target your IT accounts, or they may try and impersonate you by using a convincing looking fake email address, as the NCSC's Technical Director found out. Once they have the ability to impersonate you, a typical next step is to send requests to transfer money that may not follow due process. These attacks are low cost and often successful as they exploit the reluctance of staff to challenge a non-standard request from someone higher up in the organisation.

Good cyber security awareness throughout your organisation, security policies that are fit for purpose and easy reporting processes will all help to mitigate this risk. It is also critical that Board members understand and follow their organisation's security policies, so that when an impersonator tries to circumvent them, staff can identify that something is unusual.

You should also consider how information about you (that is publicly available) could assist an attacker who is trying to impersonate you.

What support can the NCSC provide on cyber security?

The NCSC is the UK government's technical authority and therefore takes the lead role in providing guidance and advice on cyber security for UK organisations. The NCSC:

- understands cyber security, and distils this knowledge into practical guidance that we make available to all
- responds to cyber security incidents to reduce the harm they cause to organisations and the wider UK
- uses industry and academic expertise to nurture the UK's cyber security capability
- helps organisations navigate the cyber security marketplace
- reduces risks to the UK by providing sector-specific guidance and engagement for public and private sector organisations

If you want to find out more about how you can work with the NCSC, please get in touch via enquiries@ncsc.gov.uk .

There is also government support on cyber security available from:

- Centre for Protection of National Infrastructure (CPNI) - provides advice on a range of security matters. Start with: Passport to Good Security for Senior Executives
- Department for Digital, Culture, Media and Sport (DCMS) - provides insight into the state of cyber security within the UK. Start with: FTSE350 Cyber Governance Healthcheck and the Cyber Security Breaches Survey
- National Cyber Crime Unit (NCCU) - part of the National Crime Agency and leads on investigating and prosecuting cyber crime. Start with: Cyber Threat to UK Business.

Embedding cyber security into your structure and objectives

The role of cyber security is to enable the organisation's objectives and, increasingly, enable competitive advantage. It should be adding value to your organisation rather than hindering progress. This requires a positive cyber security culture and appropriate investment and management of cyber security.

What should the Board do?

Integrate cyber security into your organisation's objectives and risks

There are two reasons why this is so important.

Firstly, cyber security impacts on every aspect of your organisation. Therefore to manage it properly it must be integrated into organisational risk management and decision making. For example:

- Operational risk will likely be underpinned by cyber security because of the reliance on the security of digital services that you use (email services, bespoke software, etc).
- Some legal risk will be tied in with cyber security risk (such as contractual requirements to protect data or partnerships, regulatory requirements to handle data in particular ways).
- Financial risk is impacted by cyber security (such as money lost through fraud enabled by cyber, revenue lost when services are taken offline by cyber attack).
- Good cyber security will also allow you to take some risk in using new technology to innovate. An overly cautious approach to risk can lead to missed business opportunities or additional (and unnecessary) costs.

Secondly, cyber security needs to be integrated for it to be successful. Good cyber security isn't just about having good technology, it's about people having a good relationship with security, and having the right processes in place across the organisation to manage it.

For example, in order to protect against an attacker accessing sensitive data (whilst ensuring that only those with a current and valid requirement can see it), you will need:

- a good technical solution to storing the data
- appropriate training for staff handling the data
- a process around managing the movement of staff, aligned with access management

Reflect this in your structure

Don't leave it to one person; Cyber security is the responsibility of the entire Board.

A cyber security incident will affect the whole organisation - not just the IT department. For example, it may impact on online sales, impact on contractual relationships or result in legal or regulatory action. There should be sufficient expertise within the Board in order to provide direction on cyber security strategy and hold decisions to account. However every member of the Board needs enough expertise to understand how it impacts specifically upon their area of focus, and to understand the broad implications for the organisation as a whole.

Cyber security outside the UK: When trying to understand the impact of cyber security on your organisation and your risks, an important consideration is which countries your organisation operates in. For those organisations who operate outside the UK or have partners outside the UK, the CPNI Smart Business Guidance highlights how this may impact your security considerations, including your cyber security. The Collaborating with suppliers and partners section of this toolkit provides guidance on how to mitigate the cyber security risk associated with these relationships.

Engage with your experts

Consider whether your reporting structure enables the Board to have the engagement with cyber security that it needs. If the CISO reports to an intermediary to the Board who has a focus on only one aspect - be that finance or legal or technology - this can potentially hinder the ability for the Board to see cyber security's wider implications. In the majority of FTSE350 organisations the CISO now reports directly to the Board.

A good place to start on improving cyber security in your organisation is to consider the communication between experts and members of the Board. Getting the structure right can help, but we also often see a reluctance from both parties to engage, because:

- technical staff think that the Board won't understand them
- the Board think that the technical staff are unable to explain the issues in the context of the strategic aims of the organisation

Improving the communication between these two groups requires effort from both sides:

- **Boards** need a good enough understanding of cyber security that they can understand how cyber security supports their overall organisational objectives
- **technical staff** need to appreciate that communication of cyber risk is a core component of their job, and ensure they understand their role in contributing to the organisation's objectives

What does good look like?

The following questions can be used to generate productive discussions with your technical team. The aim is to identify what constitutes 'good' cyber security in terms of **embedding cyber security into your structure and objectives**.

Q1. As a Board, do we understand how cyber security impacts upon our individual and collective responsibilities?

You might want to consider:

- Does every Board member have enough expertise to understand the potential impact and value of cyber security?
- Is there someone responsible for delivering the organisation's cyber security?
- Who is responsible for oversight of cyber security?
- Have we been clear about what information both the Board and our wider stakeholders need?

Q2. As an organisation, who currently has responsibility for cyber security?

This could be a person or a function, e.g. an audit committee. You might want to consider:

- How they engage with the Board - do they report directly to the Board or do they fit into another reporting process? Does this encourage the Board to actively participate in discussions on cyber security?
- What their objectives are and who sets them - do these objectives drive cyber security to be an enabler for the organisation?
- Do they have access to all the people they need to ensure effective cyber security - this could be just in terms of the resource required to meet your cyber security objectives, but could also be the teams that they need to be linked in with e.g. HR, policy, finance.

Q3. As a Board, how do we assure ourselves that our organisation's cyber security measures are effective?

You might want assurance that:

- The organisation is employing an appropriate suite of technical assurance activities and the output of this is conveyed in a meaningful way to the Board. Assurance activities might include reviewing defensive measures against suitable frameworks, such as Cyber Essentials or 10 Steps to Cyber Security.
- Threat assessments and defensive priorities are regularly reviewed and defensive measures updated accordingly.
- The focus of your cyber security measures is aligned with the risks you have identified and prioritised.

Q4. As an organisation, do we have a process that ensures cyber risk is integrated with business risk?

An example of this would be where a risk from one part of the organisation has been balanced against another. For example, an organisation may assess that introducing a Bring Your Own Device (BYOD) policy brings substantial benefit to the organisation in terms of flexible working. As part of the case for change, including assessing the business risk of not implementing a BYOD model, you would also want to:

- Assess the increase in risk associated with the increased number of devices connected to your network.
- Assess the risk associated with not owning, and therefore not being in control of, devices connected to your network.
- Consciously balance the business risks and benefits with the technical risks and benefits of BYOD.
- Consider other models, such as Corporate Owned, Personally Enabled (COPE) and compare the risks and benefits.
- Assess the suitability of planned security measures to ensure that they support rather than constrain the aims of flexible working.
- In this example, the cyber risk of introducing the new service (BYOD) has been integrated into the business risk. Those who are accountable for a service should be receiving the best possible advice, so that they can clearly balance cyber risks with other risks (and benefits) in their decision making.

Growing cyber security expertise

Cyber skills are already in high demand, and the Global Information Security Workforce study estimates that by 2022 there will a shortfall of 350,000 appropriately trained and experienced individuals in Europe. Organisations must take steps now to ensure they can draw on cyber security expertise in the future.

What should the Board do?

Baseline your current skills

The Board should have an understanding of what cyber expertise there is in the organisation and what you need. Do you have a CISO? An information security team? Incident managers? If not, should you?

This information will give you an insight into the resilience of cyber security efforts (are you currently reliant on one person?) and also will help you to understand the provenance of the cyber security information you receive.

You might also want to consider the expertise on the Board itself. Do you currently have sufficient specialist knowledge to ensure that the Board is able to make appropriate strategic decisions about cyber security? Are you likely to be able to keep pace as advances in technology bring new security challenges?

What should your organisation do?

Make an organisational plan

Given the lack of suitably skilled individuals and an increasing reliance on digital services that need to be secured, organisations that do not embrace cyber security will soon fall behind.

1. Work out what specific cyber security expertise you need. 'Cyber security' covers a range of different skills, from network security to risk management to incident response. It may be useful to first consider what skills you need to manage your highest priority objectives or risks and then assess which (if any) of these you cannot outsource and so must have in house.
2. Establish how urgently you need these skills. If you are considering developing existing staff, don't underestimate what this entails. Putting someone through a training course does not make them a cyber security expert: they must also have the opportunity to develop hands-on, practical skills and so will require support for this from within the organisation. If you need expertise in the shorter-term, it might be better to recruit a consultant or specialist.
3. Consider how you might recognise professional cyber security skills. As yet, there is no professional body for cyber security expertise (although the NCSC is working on it). This could mean that validating the ability or quality of a new hire and/or developing training plans, is difficult. Consider how you might be able to work with trusted partners or industry specialists to give you the necessary assurance.

MAKE THE BEST USE OF THE SKILLS YOU HAVE

The best way to make use of the skills you have is to identify and focus on the things that are unique to you (or the things that only people within your organisation are most qualified to do). This can be enabled by making use of established, commodity technologies. For example, you might choose to allow cloud vendors to build and secure your infrastructure, which frees your experts to spend time exploiting the unique insight they have into your organisation.

Build your best workforce: equal, diverse and inclusive

Due to the cyber security skills shortfall, your organisation must draw and nurture talent from the largest possible pool. The cyber security industry is subject to the same skills challenges as all technology-focused industries. Organisations may find it hard to recruit and retain high-calibre staff from all demographic groups. In fact there are many talented women and minorities working in cyber security, but they are often less visible. They may experience hostile working environments that slow or stop their career, or avoid the industry altogether. Working together to overcome these challenges will give your organisation a competitive edge.

LOOK BEYOND TECHNICAL SKILLS

When designing job roles and desired candidate profiles, particularly at entry level, be imaginative. Protecting our organisations relies on bringing together many different skills, technical and non-technical, to deliver security that aligns with the organisation's objectives. Recruit for broader business skills, aspiration and potential as much as for current technical skills.

LOOK AFTER YOUR EXISTING TALENT

When trying to make our organisations more diverse and inclusive, we often focus on bringing in new talent, while ignoring the issues that prevent your current staff staying and thriving once they are in. The talent available may be beyond your own direct control, but you can control how much cyber security talent you lose because of difficult policies and processes, and unwelcoming workplace cultures. As much as strong security cultures, you should focus on fully inclusive workplace cultures.

Train, buy-in, or develop for the future

Broadly there are 3 options to increase cyber expertise within your organisation.

TRAIN EXISTING STAFF

Don't just consider the staff who are already in security-related jobs. The NCSC has had huge success training staff from a variety of backgrounds, skills and experience. After all, there are many different aspects to cyber security and someone who is expert at designing a network architecture might have a very different skill set to the person working with staff to make sure security policies are practical and effective.

Depending on your organisation's needs and your staff, training could take the form of on-the-job training, professional qualifications or placements. Do remember that developing cyber security expertise is no different to many other professional areas: staff will require continuous investment, training and development opportunities to hone their expertise and also to keep up with changes in the industry.

- There are many companies who offer cyber security training. NCSC provides a list of accredited training courses.
- You could also offer time for study on an NCSC certified degree, or time for a placement on the Industry100 programme.

BUY IN EXPERTISE

There are several complementary routes available for introducing external expertise. A large organisation will probably take advantage of all of them.

1. Recruit a skilled non-executive director to your Board.
2. Employ a consultant to provide specific cyber security advice.
3. Identify specific cyber security services which can be fulfilled by a 3rd party.
4. Recruit employees who already have the skills you need.

> **Note:** good place to look for external expertise is NCSC's certified cyber professionals.

DEVELOP FUTURE STAFF: SPONSORSHIP, APPRENTICESHIPS AND WORK EXPERIENCE

Supporting young people to pursue an education in cyber security can be a brilliant way of ensuring a future pipeline of employees with the right skills. There are many schemes aimed at school and university-age students and almost all of them involve some industry participation or support, including apprenticeships, site visits and speaker opportunities.

> NCSC runs CyberFirst events and apprenticeships and is looking for company sponsors and placements. You could also forge links with universities through involvement in the CyberInvest scheme which enables organisations to fund and support cyber security research.

What does good look like?

The following questions can be used to generate productive discussions with your technical team. The aim is to identify what constitutes 'good' cyber security in terms of **growing cyber security expertise**.

Q1. As an organisation, what cyber expertise do we need, and what do we have?

You should find out:

- What expertise do we need to manage our cyber risk? What do we need to keep in-house and what can we outsource?
- Are each of our requirements continuous? For example, you might only need a penetration testing team to come in a few times a year, but you might need someone to monitor your systems all year round.
- What expertise is the minimum for all staff? How can you ensure a healthy cyber security culture in the organisation? How well and how frequently are you training staff in your security policies and any particular threats your organisation might be vulnerable to?
- How many staff do we currently have with cyber security expertise and what gaps are they telling us we have in our provision?

Q2. As an organisation, what is our plan to develop what we don't have?

You should find out:

- Which skills are a priority?
- Who owns the plan to develop cyber expertise, and how are they responsible for delivering against it?
- How you will find people with the right aptitude for the different cyber security skills? Remember that people from all backgrounds, and with technical and non-technical skills, may be well suited to this field.
- What support the Board can give to this work, both in terms of investment or broader resources?

Q3. As a Board member, do I have the right level of expertise to be accountable for cyber security decisions?

- Do I understand enough about the decisions being made on cyber security in my organisation to be accountable to shareholders?
- If not, what plan do I have in place to increase my expertise? The Introduction to Cyber Security section of this Toolkit is a good place to start. There are also many training providers who run sessions specifically for Board level.

Q4. As an organisation, are we building an equal, diverse and inclusive workforce to tackle our cyber security skills challenges?

- Do we have a champion for EDI (Equality, Diversity and Inclusion)?
- Do we have the right policies in place, and do they work well in practice as well as looking good on paper?
- Are we gathering the right data and interpreting it correctly? Are we then having the right conversations with individuals all around the organisation, to supplement this data and create a richer picture on less tangible measures?
- Are we making active, meaningful efforts to recruit from all communities, to reflect the society we operate in?
- Do we use a range of recruitment methods, to help overcome unconscious bias and ensure we fully explore candidate strengths?
- Are we confident that we are recruiting and developing staff to meet the challenges our organisation will face in the future, not just complete the tasks of today?
- Are we creating the right environment and culture to make staff feel confident, safe and comfortable in flagging issues?

Developing a positive cyber security culture

Establishing and maintaining a healthy culture, in any part of the business, is about putting people at the heart of structures and policies. However, when it comes to cyber security, there is sometimes a tendency to focus almost exclusively on the technical issues and to overlook the needs of people and how they really work.

This rarely results in success. We know, for example, that when official policy makes it hard for someone to do their job, or when a policy is no longer practical, that people find workarounds and 'unofficial' ways of carrying out particular tasks.

Without a healthy security culture, staff won't engage with cyber security so you won't know about these workarounds or unofficial approaches. So not only will you have an inaccurate picture of your organisation's cyber security, but you will also miss the opportunity for valuable staff input into how policies or processes could be improved.

What should the Board do?

Lead by example

You set the tone when it comes to cyber security. Lead by example and champion cyber security within your organisation.

We often hear stories of senior leaders ignoring security policies and processes, or of asking for 'special treatment' in some way (such as requesting a different device to those issued as standard). This tells everyone else in the organisation that perhaps you don't consider the rules fit for purpose, and/or that it is acceptable to try to bypass them.

If policies don't work for you as a Board member (that is, if you find yourself doing something different to get your job done more easily), then there is a good chance they aren't working for others either. If it seems that the policy is having a detrimental effect on the organisation, work with policy makers to adapt it.

Culture takes time and concerted effort to evolve. Don't assume that because the Board has endorsed a security posture that it will automatically cascade down throughout the organisation.

What should your organisation do?

Put people at the heart of security

Ultimately, the role of security should be to enable your organisation to achieve its objectives. It follows that if your cyber security measures aren't working for people, then your security measures aren't working.

Some organisations fall into the trap of treating people as the 'weak link' when it comes to cyber security. This is a mistake. Effective security means balancing all the different components, not expecting humans always to bend to meet the technology. More importantly, the organisation can't function with people, so staff should be supported so they can get their job done as effectively and securely as possible.

Security and leadership need to make the most of what people's behaviour is telling them. Whilst technical monitoring can look for anomalies, people can act as an early-warning system and intuitively spot something that looks unusual. Ensuring staff know who to report any concerns to can save the organisation a huge amount of time and money in the long run. If staff are working around a set procedure, this may highlight a particular policy or process that needs reviewing.

Develop a 'just culture'

Developing a 'just culture'[1] will enable the organisation to have the best interaction with staff about cyber security. Staff are encouraged to speak up and report concerns, appropriate action is taken, and nobody seeks to assign blame. This allows staff to focus on bringing the most benefit to the organisation rather than focusing on protecting themselves.

What does good look like?

The following questions can be used to generate productive discussions with your technical team. The aim is to identify what constitutes 'good' cyber security in terms of **developing a positive cyber security culture**.

Q1. As a Board member, do I lead by example?

You might do this by:

- Ensuring staff feel empowered, and have a suitable mechanism to raise security concerns, at any level in the organisation.
- Engaging with and respecting security decisions and working with decision makers to highlight ineffective policies.
- Taking responsibility for your own role in cyber security by recognising the risk you pose as a likely target for attackers and acting accordingly.
- Speaking openly and positively to staff about why cyber security is important to the organisation.

Q2. As an organisation, do we have a good security culture?

Some signs that an organisation has a good approach would be:

- Staff know how to report any concerns or suspicious activity, and feel empowered to do so.
- Staff don't fear reprisals when they report concerns or incidents.
- Staff feel able to question processes in a constructive manner.
- Staff input is demonstrably used to shape security policy.
- Staff understand the importance of cyber security measures and what it means for the organisation.

Q3. As an organisation, what do we do to encourage a good security culture?

This can vary hugely depending on the size of your organisation. Some examples we have seen include:

- Properly resourced staff awareness .
- Ensuring that staff input is included when creating new policies or system designs.
- Sharing security metrics which focus on success rather than failure (for example, how many people identified phishing emails rather than how many people clicked on them).
- Support from senior leadership on the importance of security.

[1] "A just culture is a culture of trust, learning and accountability. A just culture is particularly important when an incident has occurred, when something has gone wrong. How do you respond to the people involved? How do you minimise the negative impact and maximise learning?" – Sidney Dekker

Establishing your baseline and identifying what you care about most

There are two tasks in this section, but we examine them side-by-side as the results of one will impact on the other, and vice versa. The two tasks are:

- working out which components of your 'technical estate' (that is, your systems, data, services and networks) are the most critical to your organisation's objectives
- understanding what your technical estate comprises, so that you can establish a baseline which will inform both your risk assessments and the deployment of your defensive measures

Whilst these two tasks have separate purposes, you will need to have some baseline of your technical estate in order to understand which parts of it are mission critical. At the same time, you will need some way to prioritise which areas to baseline, as doing this for your entire technical estate would be a very resource intensive task.

What should the Board do?

Work out what you care about the most

As with any other business risks, your organisation will not be able to mitigate all cyber security risks at all times. So the Board will need to communicate key objectives (it might be 'providing a good service to customers and clients', for example) in order for the technical experts to focus on protecting the things that ensure these objectives are fulfilled.

The Board should also consider what is most valuable to the organisation. For example, the Board might know that a specific partner is crucial to the organisation and that a compromise of their data would be catastrophic. This should be communicated to technical teams, so that they can prioritise protecting these 'crown jewels'.

It is **critical** that this is an active and ongoing discussion between Boards and their experts:

- Boards will have business insight that technical teams may not have (such as which particular partner relationship must be to be prioritised)
- technical teams will have insight into the enablers for key objectives (such as which networks or systems do particular partners rely upon)

Only by bringing these two together can you get a full picture of what is important to protect. Once you have this picture it is likely the Board will still need to prioritise within that list. This understanding will not only help focus the aim of your cyber security, but will also inform the assessment of the threat your organisation might be facing.

What are your crown jewels? Your crown jewels are the things most valuable to your organisation. They could be valuable because you simply couldn't function without them, or because their compromise would cause reputational damage, or it would incur financial loss. Some examples could be:

- bulk personal data
- intellectual property
- your public-facing website
- industrial control systems

What should your organisation do?

Work out where you are starting from

This provides information that underpins your risk decisions in two ways.

Firstly, it influences the options you have. Knowing which systems are connected to each other, who and what has access to particular data, and who owns which networks are all critical to setting good defences. This information will also be required in an incident to make an assessment of the damage an attacker could be inflicting, or the impact of any remedial actions you might decide to take.

Secondly, it might influence your risk assessment. Sometimes a risk comes not from a threat to an important asset, but from a vulnerability in your organisation's systems. Many incidents are the result of vulnerabilities in older, legacy systems, and the incidents arise not because the vulnerability can't be defended against, but because the organisation didn't have a good enough understanding of their systems to realise they were exposed.

Understanding the entirety of your estate can be a daunting, or impossible, task - especially for organisations whose networks and systems have grown organically - but even a basic understanding will help, and a good understanding of your priorities can help focus this task.

Identify critical technical assets

Based on the Board's priorities you need to identify what parts of the technical estate are critical to delivering those top-level objectives. This could be systems, data, networks, services or technologies. For example, maintaining a long-term customer base may be a priority objective. There are lots of ways that good cyber security could enable this. It could be:

- securing a customer database to protect their data
- ensuring resilience of the order processing system to ensure deliveries go out on time
- ensuring availability of the website so that customers can contact you easily

It can sometimes be difficult to identify these dependencies as they are such an integral part of your operation that they can be taken for granted, but the questions below can help. Doing this in conjunction with baselining your technical estate will also help to potentially identify assets that you weren't even aware of, and are actually critical to providing certain services.

Working with suppliers and partners Most organisations will have suppliers or partners with whom they receive, provide or share information, systems or services. You must consider this in your baseline of your estate as these are potential entry points to your organisation.

What does good look like?

The following questions can be used to generate productive discussions with your technical team. The aim is to identify what constitutes 'good' cyber security in terms of **establishing your baseline and identifying what you care about most**.

Q1. As an organisation, do we have a clear understanding of how technical systems, processes or assets are contributing to achieving our objectives?

Some questions to consider that may help in identifying these dependencies include:

- What are our 'crown jewels' (that is, the things our organisation could not survive without) ?
- What requirements must we meet (such as legal or contractual requirements) ?
- What do we not want to happen, how could that come about ?

Q2. As a Board, have we clearly communicated our priority objectives and do we have assurance that those priorities guide our cyber security efforts?

Cyber security strategy should be integrated into your organisation's strategy and your strategic priorities should guide defensive efforts. A good organisation should have a process for ensuring these strategies remain aligned and should be able to demonstrate how investment is focused on those priorities.

For example, if a promise to customers about their privacy is a priority then you might:

- identify what could jeopardise this promise e.g. the loss of their credit card details
- identify what technical assets are required to secure those details e.g. database, access management system
- prioritise defending these assets when implementing cyber security measures
- audit measures regularly

Q3. As an organisation, how do we identify and keep track of systems, data or services that we are responsible for?

If you are a large organisation and your systems have grown organically, understanding the detail of your systems, devices and networks may be impractical. At a minimum you should be aware of what level of understanding you do have and the potential risks that any undocumented systems might pose. Ideally you want to start with a good idea of what your technical estate looks like and then have a process to ensure any changes are considered and recorded to keep the baseline up to date. This baseline might include information such as:

- inventory of the hardware and software used across the organisation
- an up to date register of systems, including all internet-connected, partner-facing, systems and networks
- details of data sets; which services, systems and users have access to them, where are they stored, how are they managed

Understanding the cyber security threat

The type of threat faced is shaped by the nature of organisation and the services an organisation provides. For example, the vast majority of organisations won't be targeted specifically by nation states and so may focus on the threats posed by cyber criminals. However, organisations who form part of, or are providing services to, our Critical National Infrastructure and defence sector may be at risk from nation states.

Understanding the threats faced by your organisation, either in its own right or because of who you work with, will enable you to tailor your organisation's approach to cyber security investment accordingly. You need to consciously make the decision about what threat you are trying to defend against, otherwise you risk trying to defend against everything, and doing so ineffectively.

What should the Board do?

Get an understanding of the threat

An understanding of the cyber security threat landscape will be key to helping the Board make well-informed governance decisions. For example, you may prepare differently for a merger with a company if you know that they provide important products or services to Critical National Infrastructure and therefore may be a target for a nation state. The Board will already have insight into the threats or challenges facing their sector. This should be complemented by an awareness of the motivations of attackers, and a mechanism for staying up to date with key cyber security developments (for example, the growth of ransomware).

Collaborate on security

One of the best sources of information on good practice and relevant threats can be your sector peers. Attackers often target a number of organisations in the same sector in a similar manner. Cultivating these collaborative relationships on security has two major benefits. Firstly, it can help make your own organisation more resilient, through early warning of threats and improved cyber security practice. Secondly, it helps make the sector as a whole more resilient, which can reduce the appeal to potential attackers.

> **Cyber Security Information Sharing Portal**: The NCSC's Cyber Security Information Sharing Partnership provides a secure forum where companies and government can collaborate on threat information. Access to CISP not only provides the opportunity to securely share intelligence with trusted partners in your sector, but also gives access to sensitive threat reports and the full breadth of NCSC advice.

Assess the threat

Working out the 'threat actors' (the groups or individuals capable of carrying out a cyber attack) relevant to your organisation can help you make decisions on what you are actively going to defend against. Whilst investing in a good baseline of cyber security controls will help defend your organisation from the most common threats, implementing effective defences against a more targeted or sustained attack can be costly. So dependent on the likelihood and impact of that threat, you may decide that it is not worth that additional investment.

Ongoing discussion between the Board and experts will help you to prioritise the threats to actively defend against. The experts will have an in-depth understanding of the threat, and the Board will be able to identify the features of the organisation that might make it an attractive target to attackers. It is also critical to have this discussion in advance of any decision that will significantly change the threat profile of the organisation, in order to give technical staff the time to suitably adapt the organisation's cyber security.

Working with suppliers and partners

When assessing the threat, you should consider not only the value that you might have as a standalone organisation, but also the value you may represent as a route into another, possibly larger organisation. For example, you may supply important services to an organisation involved in Critical National Infrastructure, in which case, a nation state may want to attack your organisation in order to access their ultimate target.

What should your organisation do?

Don't underestimate the impact of untargeted attacks

An untargeted attack is where an attacker uses a 'scattergun' approach to reach thousands of potential victims at once, rather than targeting a specific victim. Attackers often use automated, widely available tools that scan public-facing websites for known vulnerabilities. This same tool will then, once a vulnerability has been found, exploit that website automatically, regardless of who it belongs to. This could have just as much impact on your organisation as a targeted attack. A good baseline of basic cyber security controls and processes will protect your system from the majority of these attacks.

Obtain good intelligence - and use it

You will need different types of threat intelligence for different purposes. A good overall threat picture is needed for governance decisions and timely threat intelligence for day-to-day and tactical decisions. Many industry and government partners offer threat intelligence, from annual reports on general trends, right down to highly technical reports on a specific type of malware. You therefore need a mechanism for identifying what intelligence your organisation needs, for what purpose and for sharing that intelligence internally. Critically you then need to use that intelligence to inform business decisions, including procurement, outsourcing, training, policy and defence of your networks.

You can also gather threat intelligence internally. You will likely have experience of attacks on your own organisation which can provide strategic insight into activities of threat actors, as well as tactical details on the methods of the threat actors. These specific details will likely come from logging or monitoring within your organisation.

What does good look like?

The following questions can be used to generate productive discussions with your technical team. The aim is to identify what constitutes 'good' cyber security in terms of **understanding the cyber security threat to your organisation**.

Q1. As an organisation, which threats do we assess are relevant to our organisation, and why?

This assessment should:

- identify potential motivation for those threats and the likelihood of them targeting your organisation
- inform which risks you are willing to tolerate
- be enriched by collaboration with key partners in your sector
- be supported by evidence from the attacks you have experienced to date

Q2. As an organisation, how do we stay up to date with the cyber threat?

You might:

- seek to discover evidence of any attacks in system logs you may hold
- subscribe to a number of threat intelligence feeds
- be part of a sector-specific intelligence sharing group
- have mechanisms for sharing key cyber threat updates internally

Q3. As an organisation, how do we use threat intelligence to inform business as usual (BAU)?

This should be a continuous cycle with threat assessments informing BAU decisions, and BAU experience informing the threat assessments. Examples might be:

- assessing the likelihood and impact of threats to inform risk assessments and appetite
- educating staff on the key threats they face so that they can make informed decisions
- taking lessons from previous incidents to inform threat assessments
- using threat intelligence to focus defensive measures
- including threat consideration in change or procurement decisions (for example, when choosing a new enterprise IT provider, considering a potential merger or designing a new product)

Risk management for cyber security

Most organisations will already be taking steps to assess and manage their cyber security risk. However it is worth considering what the driver is for that activity. Often, organisations conduct risk management exercises for 'compliance' reasons, which could include:

- obligations from external pressures (such as regulatory requirements)
- customers' demands
- legal constraints

When done for these reasons, there is a danger of risk management becoming a tick-box exercise. This can lead to organisations believing they have managed a risk, when in reality they have merely complied with a process which may have (albeit unintended) negative consequences.

Compliance and security are not the same thing. They may overlap, but compliance with common security standards can coexist with, and mask, very weak security practices. Good risk management should go beyond just compliance. Good risk management should give insight into the health of your organisation and identify opportunities and potential issues.

What should the Board do?

Integrate cyber security into organisational risk management processes

Many of your organisational risks will have a cyber component to them. Cyber security risk should therefore be integrated with your organisational approach to risk management. Dealing with cyber security risk as a standalone topic (or considering it simply in terms of 'IT risk') will make it hard for you to recognise the wider implications of those cyber security risks, or to consider all the other organisational risks that will have an impact on cyber security.

The role of cyber security should be to support and enable the business, and it should do this by managing its risks without blocking essential activities, or slowing things down, or making the cost of doing business disproportionately expensive.

Don't make reducing risk levels the measure of success

It can be difficult to measure the success of your organisation's cyber security efforts. A typical output of good cyber security is the absence of a failure, which can be hard to measure, and since cyber security is still a relatively new field there aren't yet many established metrics to draw on.

It is common for risk assessments to deliver some kind of assessment level, be that high medium low, or a number, and so it could be tempting to use this as a performance metric for your cyber security efforts. However, they are a poor metric of your internal security efforts as they are influenced by external factors that are outside of your control - factors which change extremely rapidly. New vulnerabilities are being discovered every day and the number of actors seeking to use cyber means to achieve their aims is increasing.

Driving performance through reduction of a number associated with the cyber security risk will likely incentivise risk assessors and reviewers to underestimate the risks, leading to less informed decisions. Some considerations on what 'good metrics' look like is provided in Implementing effective cyber security measures.

What should your organisation do?

Be realistic about the risks

Similar 'good practice' risk management principles will apply for managing cyber risk as they would for managing any other organisational risk. However, there are two things to bear in mind.

Firstly, solutions and technologies in cyber security are advancing so quickly that it is easy to get caught out using outdated assessments of cyber risks. So you may need to review cyber security risks more regularly than other risks.

Secondly, because cyber security is still a relatively new field, the organisation won't have as intuitive an understanding of cyber security risks, as it might for say, financial risk. As new technologies emerge, there might not be a huge evidence base to draw on to form a risk assessment. This is worth bearing in mind when considering the confidence you have in an assessment of cyber security risk, especially if that assessment is going to be directly compared to assessments of more well-established risks.

A good example of this is cloud security. The NCSC see many organisations hesitant to use cloud services because they intuitively assume it is high risk, informed mainly by the belief that storing something valuable with a third party is more risky. In reality, the third party (so in this case a cloud service provider) may have better security measures within their data centres than your own on-site storage. So the overall risk may actually be lower. A decision to adopt recent technologies - like cloud storage - would need to be based on a comprehensive understanding of all the risks, rather than an intuitive assessment.

Managing risk for newer technologies The NCSC has produced guidance on Cloud security and Software as a Service which can help identify and assess the associated risks.

What does good look like?

The following questions can be used to generate productive discussions with your technical team. The aim is to identify what constitutes 'good' cyber security in terms of **managing cyber security risk**.

Q1. As an organisation, do we have a process that ensures decision makers are as well informed as possible?

The primary focus of your process should be that decision makers can make the most well-informed decisions. The decision makers might be the Board (who have to set a risk appetite based on an understanding of a technical or operational risk) or it might be the practitioners who need to decide how to implement a specific course of action fed down from the Board. Both need to be as well informed as possible (in an understandable format) to allow those decisions to be made well. This means the output of risk assessments needs to **meaningfully** articulated. Qualified outputs are usually the most effective and are preferable to meaningless results where sometimes arbitrary numbers are added or multiplied to derive a score.

Q2. As an organisation, do we have a process that ensures cyber risk is integrated with business risk?

Any decision maker in your organisation should have an awareness of the importance of cyber security risk and enough expertise (or access to expertise) to consider cyber security risk in the decisions they make. To begin with you might want to:

- consciously build in consideration of cyber security risk to any decision making processes you have
- focus on educating people on cyber security

A way to check if this is working is to look at a decision taken in your organisation and review whether cyber security risk has been balanced with other business risks. For example, an organisation may assess that introducing a Bring Your Own Device (BYOD) policy brings substantial benefit to the organisation in terms of flexible working. There are many different things you would expect to be considered in this decision, including:

- the potential improvement in staff productivity
- the potential security implications of having devices the organisation does not control connecting to the organisation's networks
- the cost implications
- the liability implications

Were these considered jointly when making the decision, or was security only discussed once the decision was already made?

Q3. As an organisation, do we have an effective and appropriate approach to manage cyber risks?

Both the Board and the practitioners should be able to clearly and simply articulate the process in a few minutes. The details of this framework might include:

- how risks are escalated
- what the threshold is for Board involvement in a risk decision
- how we convey the confidence in a particular risk assessment
- how often risks are reviewed
- who owns which risks
- who is responsible for the framework itself and for ensuring it is fit for purpose (for example, ensuring that the output of the risk assessment process genuinely reflects the assessment of the risk)

Q4. As a Board, have we clearly set out what types of risks we would be willing to take, and those which are unacceptable?

- Support decision makers if they make risk decisions within the parameters you set.
- Be clear on the process and the threshold for escalating the risk.
- Be as specific as you can in terms of the types of risk and the amount of risk. For example, you might be unwilling to tolerate any significant risk to personal data but would be willing to accept email being unavailable for a day.
- Consider the cumulative risk you are accepting; it's possible that all your cyber risk could be realised at the same time. In a single incident, you might lose email for a day, the public website might be unavailable and financial data you hold might be stolen. Whilst you may have accepted some risk of all those things happening, you may not have considered whether the organisation could tolerate them all happening at once.

Implementing effective cyber security measures

Implementing good cyber security measures is not only a key part of meeting your regulatory requirements but will also help reduce the likelihood of a significant incident. Implementing even very basic cyber security controls will help reduce the chance of an incident.

5 questions for the boardroom agenda If you'd like more details about how to generate constructive cyber security discussions between board members and technical experts, refer to the NCSC's original 'Board toolkit: five questions for your board's agenda' guidance.

What should the Board do?

Get a little bit technical

Having a basic understanding of cyber security can help you to ask the right questions to seek assurance about your organisation's cyber resilience - just as you would need to have a certain level of understanding of finance to assess the financial health of your organisation. A good place to begin is to discuss your existing cyber security measures with your experts, and the questions below suggest a starting point for what to ask.

What should your organisation do?

Start with a cyber security baseline

Attackers often use common methods to attack a network. A lot of these methods can be mitigated against by implementing basic cyber security controls. There are several frameworks that outline what good cyber security controls look like. These include ISO/IEC 27002, the NIST Cyber Security Framework and the NCSC's 10 Steps to Cyber Security, a summary of which is shown below.

If you are an SME or a charity with fewer resources available to combat cyber security, you may want to instead use the Small Business Guide or Small Charity Guide.

Tailor your defences to your highest priority risks

The basic cyber security controls will help mitigate against the most common cyber attacks, but once you have that baseline in place, you then need to tailor your defences to mitigate your highest priority risks. Your measures will be tailored both to your technical estate (protecting the things you care about the most) and to the threat (protecting against methods used by specific threat actors).

NCSC guidance can help you address these priorities. For example, if you know that one of your critical systems has external connections, you might consider the specialised guidance on how to safely import data into that system.

Layer your defences

As with physical and personnel security, cyber security can make use of multiple measures which (when implemented simultaneously) help reduce the chances of single point of failure. This approach is commonly referred to as 'defence in depth'. Each measure provides a layer of security and deployed collectively, greatly reduce the likelihood of a cyber incident. Once you have your cyber security baseline in place you can focus on layering your defences around those things that are most important to you - or particularly valuable to someone else.

Defend against someone inside your network

Defences do not stop at the border of your network. A good defence assumes that an attacker will be able to access your system and works to minimise the harm that they can do once they are inside it. One of the key things you can do to limit the damage they can inflict is to restrict their movement and access. Effectively managing user privileges and segregating your network are common approaches. Identifying an attacker inside your system as soon as possible will also help limit the damage they can do. Monitoring and logging are key to being able to spot any signs of malicious activity.

These measures will also help mitigate the threat from a malicious insider; somebody who has legitimate access to your systems but then uses that access to do harm. This threat ranges in capability and intent, from a disgruntled employee through to corporate espionage.

Review and assess your measures

Good cyber security is a continuous cycle of having the right information, making informed decisions and taking action to reduce the risk. You will need to be continuously assessing and adapting your defences as the needs of your organisation and the profile of the threat changes. To do this it's important to have some way to assess whether your defences are effective.

There are several mechanisms available to technically assess the effectiveness of your security controls. This may include things like testing the security of your networks (pen-testing) through to certification of products or services. You may want to use a combination of internal mechanisms and objective assessment provided by an external source.

Engaging with staff will also help you gain a more accurate picture of your organisation's defences. It will also give you the opportunity to get valuable staff input into how policies or processes could be improved. Metrics or indicators can also tell you where you need to change your approach or adapt to new circumstances. Understanding exactly what an indicator is telling you may require further investigation of the situation. An example is the trend in people reporting suspicious emails. A decline in the number of people reporting can either mean fewer malicious emails are getting through to people's inboxes, or it could mean fewer people are reporting any concerns because they don't receive feedback when they do, and therefore believe nothing is ever done afterwards.

What does good look like?

The following questions can be used to generate productive discussions with your technical team. The aim is to identify what constitutes 'good' cyber security in terms of **assessing your organisation's cyber security measures**.

Q1. As an organisation, how do we assure ourselves that our measures are effective?

You might seek this assurance through:

- Penetration testing carried out by an external organisation, and action taken on the back of their results.
- Automated testing of your defences and monitoring of activity on your networks by your IT security team.
- Reviewing defensive measures against suitable frameworks, this could be an internal review or an independent consultant. Suitable frameworks might be Cyber Essentials, 10 Steps to Cyber Security, ISO/IEC 27002 or the NIST Cyber Security Framework.
- Ensuring threat assessments and defensive priorities are regularly reviewed and defensive measures updated accordingly.
- Ensuring that the focus of your cyber security measures is aligned with the risks you have identified and prioritised.

Q2. As an organisation, what measures do we take to minimise the damage an attacker could do inside our network?

You might consider:

- How you authenticate and grant access to users or systems. You want to ensure that these measures are not easy to bypass and that you don't afford access unless necessary.
- How you would identify an attacker's presence on your networks - normally done through monitoring.
- How you separate your network so that if an attacker gets access to one device they do not have access to the full range of your technical estate.

Further details on these three points are provided in NCSC guidance on preventing lateral movement.

Q3. As an organisation, do we implement cyber security controls to defend against the most common attacks?

As an organisation, how do we defend against phishing attacks?

- We filter or block incoming phishing emails.
- We ensure external mail is marked as external.
- We stop attackers 'spoofing' our own emails.
- We help our staff to identify and report suspicious emails.
- We limit the impact of phishing attacks that get through.

As an organisation, how do we control the use of privileged IT accounts?

- We use 'least privilege' when setting up staff accounts.
- We reduce the impact of attacks by controlling privileged accounts.
- We have strong links between our HR processes and the IT account function.

As an organisation, how do we ensure that our software and devices are up to date?

- We have defined processes to identify, triage, and fix any exploitable vulnerabilities within our technical estate.
- We've created an 'End of life plan' for devices and software that are no longer supported.
- Our network architecture minimizes the harm that an attack can cause.
- We make appropriate use of 3rd party or cloud services and focus on where we can have most impact.

As an organisation, what authentication methods are used to control access to systems and data?

- We take measures to encourage the use of sensible passwords.
- We ensure passwords don't put a disproportionate burden on staff.
- We implement two factor authentication (2FA) where possible.

Collaborating with suppliers and partners

There are four reasons why cyber security is a key consideration when collaborating with suppliers and partners:

1. You increase the number of routes and external touchpoints in your organisation. So if any of them are compromised, you are also at risk.
2. You may be targeted as a way into the organisation you are supplying.
3. Your suppliers may be targeted as a route into your organisation.
4. You may be sharing sensitive or valuable data or information that you want suppliers to protect.

Being able to demonstrate a good level of cyber security is increasingly a key component of supplier and provider contracts, and is already a requirement for many government contracts.

What should the Board do?

Build cyber security into every decision

All organisations will have a relationship with at least one other organisation, be that the provider of your email service, or the developers of the accounting software you use, through to your traditional procurement supply chain. Most organisations will be reliant on multiple relationships. Each of these relationships will have a level of trust associated with them, normally some form of access to your systems, networks or data. There are three key things you therefore need to ensure:

1. That this access doesn't provide a route for an attacker to gain access to your organisation, either through deliberate action or unintentional consequence.
2. That any partner or supplier is handling any sensitive data appropriately and securely.
3. That any product or service you buy has the appropriate security built in.

Cyber security risk should be a key consideration in any decision on new relationships or collaborations. This includes decisions on suppliers, providers, mergers, acquisitions and partners.

What should your organisation do?

Identify your full range of suppliers and partners, what security assurances you need from them, and communicate this clearly

Review your current supply chain arrangements to ensure you are setting out your security needs clearly and identifying the actions you need to take as a result. If you yourself are a supplier, ensure you meet the security requirements set for you by your customer as a minimum.

Ensure that the security requirements you set are justified and proportionate and match the assessed risks to your operations. Also be mindful of the current security status of your suppliers to give them time to make the necessary improvements. It might be useful to include references to the following NCSC guidance that can help to establish a baseline of cyber security:

- 10 Steps to Cyber Security
- Small Business Guidance
- Cyber Essentials

The following NCSC guidance can help you to assess your own security needs from suppliers:

- Supply chain guidance
- Cloud services guidance
- Software as a Service guidance

Get assurance

Security should be built into all agreements from the start, and you should have confidence that your security needs are being met. Dependent on your relationship with the supplier or provider and your resources, you could seek assurance of this through testing, auditing or adherence to accreditation standards.

Consider the implications if your supplier is compromised

No matter how comprehensive your security agreements with your partners are, and no matter how well they implement their controls, you should assume that your partners will be compromised at some point. You should plan the security of your networks, systems and data accordingly with this assumption in mind. This is also worth considering in your security agreements; what are you expecting of them and their response? Do they have to notify you? Do they have to assist you if you are consequently also compromised?

What does good look like?

The following questions can be used to generate productive discussions with your technical team. The aim is to identify what constitutes 'good' cyber security in terms of **assessing your organisation's cyber security measures**.

Q1. As an organisation, how do we mitigate the risks associated with sharing data and systems with other organisations?

You should:

- Have a good understanding of your suppliers, what data and networks they have access to and have a process for keeping this up to date.
- Set clear expectations of how your partners protect your data and access your systems.
- Build security into all relationships and agreements from the start.

To do this you might:

- If you have a very large number of supply chain companies, agree processes with your main suppliers on how they sub-contract any work, specifically what obligations they have to inform you.
- Choose organisations that can demonstrate the security of their defences. For example, larger organisations will have carried out regular pen tests and responded to the findings to understand their residual vulnerability. SME's might have been certified under the government's Cyber Essentials Scheme.
- Limit services exposed and information exchanged with other organisations to the minimum necessary.
- Implement user and system authentication and authorisation before access is granted.
- Audit any sensitive actions or data exchange/access.

Q2. As an organisation, how do we ensure that cyber security is considered in every business decision?

Security should be embedded in your culture and strategy, and should therefore be consciously considered in any decision regarding procurement, mergers or acquisitions. If there is a process for making those decisions, security can be explicitly identified as a relevant consideration and any conclusions recorded.

Q3. As an organisation, are we confident that we are fulfilling our security requirements as a supplier?

If you are a supplier to other organisations you are exposed to an increased risk. Both a reputational risk (if your product causes your customer to be compromised) and also operational risk (since you now provide access to more, and potentially more valuable, organisations). You should:

- Know how you would respond should your organisation be compromised, putting at risk partner networks you are connected to, or customer data you may hold.
- Have a good understanding of your customers and the impact they may have on your threat profile (for example, if you are in the supply chain for UK Critical National infrastructure you may be at increased risk from foreign state actors).

Q4. As a Board, do we have a clear strategy for using suppliers, and have we communicated it?

If procurement and supplier decisions are devolved below the Board, have you clearly described:

- What risk you are willing to accept in using suppliers? For example, if your organisation is compromised through a supply chain attack, you may not be exposed to the same level of reputational risk as if you were directly compromised, but you may be exposed to the same level of financial risk.
- What are your expectations of suppliers' security, and how much you are willing to pay for better security? For example, if company A is more expensive but also more secure, how much cheaper would company B need to be to make it the better option?
- What opportunities you are trying to exploit? This should be supported by an awareness of what you are able to cater within your organisation and what you will outsource. For example, if you assess it's not feasible to support your own data storage, do you take advantage of the competitive cloud data storage market?
- What your appetite is for working with partners or suppliers overseas? Some jurisdictions are incompatible with UK security and regulatory requirements or may bring very different continuity of supply issues. For further considerations see CPNI's Secure Business guidance.

Planning your response to cyber incidents

Incidents can have a huge impact on an organisation in terms of cost, productivity and reputation. Being prepared to detect and quickly respond to incidents will help to prevent the attacker from inflicting further damage, so reducing the financial and operational impact. Handling the incident effectively whilst in the media spotlight will help to reduce the impact on your reputation.

Experiencing an incident? If you are currently experiencing an incident, you can contact the NCSC.

What should the Board do?

Ensure you have a plan

1 in 10 organisations don't have an incident management plan. If you're one of these organisations, then you should address this immediately.

Understand your role in incident management

Incidents often occur at inopportune moments and most people's decision making is compromised in times of crisis. For these reasons, everyone must have a clear understanding of their role and the organisational response in advance, especially Board members who would likely be representing the organisation in the media.

The Board also needs to be explicit about who it is willing to devolve authority to (especially outside core working hours), and exactly what that authority covers. For example, does that cover calling in a contracted incident response company, or taking down a public facing website? The Board also needs to be explicit about when it wants to be informed of an incident, both in terms of at what stage of the incident, and in terms of what significance of incident they need to know about.

Get involved in exercises

The best way to test these processes and thresholds (and to get a good understanding of the Board's role) is through exercising the incident management plan. If you would be involved during a real incident, then you should be involved in an exercise. Doing this in conjunction with operational staff can also help to highlight issues around authority for critical decisions. Even if you do not have a direct role in responding to an incident, running an exercise can be a good way to understand the realities of how an incident would impact on your organisation.

Drive a 'no blame' culture

Post-incident analysis provides insight that can help you reduce the likelihood of incidents occurring in the future and reduce their potential impact. Crucially in order to get this insight you need to be able to be honest and objective about what has happened. This can only happen in a no blame culture, such as you would use when investigating health and safety incidents. Critically for the Board, new regulation, such as GDPR, is clear that responsibility for incidents or data breaches sits with the organisation and not an individual. Therefore the Board is ultimately responsible for any cyber security incident as the governing body. Apportioning blame to a specific individual within the organisation will be treated as poor cyber security practice.

What should your organisation do?

Work out what an incident would look like

One of the most common things overlooked is being able to identify what constitutes an incident. There's two aspects to this:

- working out how you would spot an event in the first place
- working out at what point an event (something happening on your networks or systems) becomes an incident

HOW WOULD YOU SPOT AN EVENT?

Depending on their motives, an attacker is unlikely to tell you when they have successfully compromised your organisation, so you need your own methods to identify an intruder or an attack. This normally takes the form of monitoring. Monitoring refers to observing data or logs collected from your networks or systems to identify patterns or anomalies that could indicate malicious activity. Even if you don't have monitoring to identify the incident, it is still useful to collect system or network logs (especially those relevant to your critical assets) so that you can retrospectively review them once you know an incident has occurred.

WHEN DOES AN EVENT BECOME AN INCIDENT?

This is often not a clear cut decision. You can try and gather as much information as possible to inform your assessment of an 'event', but you probably won't have a complete picture of what has happened. Beginning an incident response might have implications for cost, reputation and productivity, so you will want to consider who has the authority to make this decision, and what the thresholds are for an incident in advance.

WHAT IS A CYBER SECURITY INCIDENT?

A breach of the security rules for a system or service - most commonly:

- attempts to gain unauthorised access to a system and/or to data
- unauthorised use of systems for the processing or storing of data
- changes to a systems firmware, software or hardware without the system owner's consent
- malicious disruption and/or denial of service

Use the information you already have

All the information you have previously gathered on what's important to protect, the threat and your technical estate will provide critical insight in two key areas:

- It will give you insight into the impact of incident. If the attacker has accessed a particular user device, what could they access? Could they access those things you care about the most?
- It will help you determine your operational response. If the attacker is on a specific network can you isolate that network? If you can, what would the impact be on your organisation?

Take pre-emptive measures

Put measures in place to help reduce the harm that an attacker could do. This could be:

- introducing measures that restrict their movement once they are inside your network
- pre-emptively reducing the impact of attacks (for example, backing up your data will help to reduce the impact of a ransomware incident)

As with any other defensive measures, these should be focused on protecting what is most important to you.

Make an Incident Management plan

Cyber Incident Response is a complex subject as no two incidents are ever the same. However, as with all business continuity planning, you can develop a plan that will outline the key elements of your response. Your plan should not only cover the technical elements, but also:

- the people and process elements such as media, customer and stakeholder handling
- reporting to regulators
- dealing with legal actions

For more common incidents (such as DDOS) it may be helpful to develop a specific 'playbook' setting out your organisation's response.

Test your plan

Rehearsing your response to different scenarios is key to ensuring your plans are effective and remain current. There are various exercising packages you can use. This will be a critical part of the role for any staff involved directly in incident management, but every Board member also needs to understand their specific area of responsibility during an incident.

Learn lessons

An often overlooked aspect of incident management is the post-incident review. An incident can provide valuable insight into your cyber readiness, including:

1. The threat your organisation faces.
    - Who carried out the attack and was it targeted?
    - Did they go about it in the way you expected?
    - Did they go after the things you expected?
2. The effectiveness of your defensive measures.
    - What did your defences protect against?
    - What didn't they?
    - Could they be improved?
3. The effectiveness of your incident response measures.
    - What would you have done differently?
    - Did your response help to reduce the impact of the incident?
    - Did it make some aspects worse?

Working with suppliers and partners Your plan should also consider how you mitigate the impact on any partners or customer organisations if you were compromised. When do you inform them? What mechanisms are in place to limit the damage it could do to them? You should also consider what you would do in the event that a supplier is compromised; you may not have control over how they deal with the incident. What would you be able to do independently to reduce the impact on your organisation? The best way to mitigate this risk is to have a collaborative approach to your security with your partners and suppliers.

What does good look like?

The following questions can be used to generate productive discussions with your technical team. The aim is to identify what constitutes 'good' cyber security in terms of **responding to cyber incidents**.

Q1. As an organisation, do we have an incident management plan and how do we ensure it is effective for cyber incidents?

A basic plan should include:

- Identifying the key contacts* (incident response team or provider, senior management, legal, PR, and HR contacts, insurance providers).
- Clear escalation routes (for example to senior management) and defined processes for critical decisions.
- Clear allocation of responsibility (specifically whether this is for normal working hours or 24/7).
- Basic flowchart or process for full incident lifecycle .
- At least one conference number which is available for urgent incident calls.
- Guidance on regulatory requirements such as when incidents need to be reported and when to engage legal support.
- Contingency measures for critical functions.

Q2. As an organisation, do we know where we can go for help in an incident?

This might include:

- Incident response providers (you might want to consider NCSC Certified Incident Response companies)
- NCSC Incident Management team, or if you believe you have been the victim of online fraud, via ActionFraud.
- Intelligence sharing groups, for details of other companies experiencing the same incident (consider joining CISP).

Q3. As an organisation, do we learn from incidents and near misses?

It's important to learn lessons from incidents as well as from 'near-misses'. These will give you valuable insight into the threat you're facing, the effectiveness of your defence, and potential issues with your policies or culture. A good organisation will use this insight to respond better to future incidents, and not seek to apportion blame. The Board may decide it doesn't need to know the details of every incident, just the most significant lessons learned from the incidents experienced.

Q4. As an organisation, how would we know when an incident occurred?

This incorporates two aspects; what are the triggers that can tell us an incident has happened, and how do we then share that information within the organisation?

When considering what might trigger an incident, you need to consider:

- What monitoring is in place around critical assets (like personal data) that would have an impact if compromised, lost or changed?
- Who examines the logs and are they sufficiently trained to identify anomalous activity?
- What reporting mechanisms are there in place for staff to report any suspicious activity?
- Are the thresholds for alerts set to the right level - are they low enough to give suitable warning of potential incidents and high enough that the team dealing with them are not overloaded with irrelevant information?

When considering how an incident will be shared internally, consider:

- What constitutes an incident?
- Who has the authority to make that decision?
- Who needs to know the details of the incident?
- Has the Board explicitly conveyed the threshold for when it wants to be informed of an incident?

Q5. As a Board, do we know who leads on an incident and who has the authority to take any decisions?

This will depend on your organisational structure. It might sit with the one member of the Board, or one of the executives, or it might be divided out into different roles. Ideally you should:

- Specify exactly who is able to take decisions on which aspects.
- Have backup plans in place if those decision makers are unable to fulfil that duty (for example, out of hours).
- Test this decision-making process, with a focus on potential areas of overlapping responsibility.

Q6. As a Board member, do I understand what's required of my role during an incident, and have I had training to equip me for that role?

Consider:

- Do I have the understanding required to make decisions potentially out of hours, and under time pressures?
- Do I need training to support my specific role in an incident, such as understanding relevant regulation, or dealing with the media?

Appendices

Appendix 1: Cyber security regulation

The regulation summarised below outlines the need for organisations to demonstrate and implement cyber security standards. The NCSC has contributed to the setting of cyber security standards to ensure they reflect good cyber security practice. By following and implementing NCSC guidance, organisations will be 'on their way' to meeting the cyber security requirements regulation.

General Data Protection Regulation (GDPR)

The GDPR requires that personal data must be processed securely using appropriate technical and organisational measures. The Regulation does not mandate a specific set of cyber security measures, but rather expects you to take 'appropriate' action. In other words you need to manage risk. What is appropriate for you will depend upon your circumstances, as well as the data you are processing and therefore the risks posed.

However, there is an expectation you have minimal, established security measures in place. The security measures must be designed into your systems at the outset (referred to as Privacy by Design) and maintained effective throughout the life of your system.

The NCSC have worked with the ICO to develop a set of GDPR Security Outcomes. This guidance provides an overview of what the GDPR says about security, and describes a set of security related outcomes that all organisations processing personal data should seek to achieve.

Networks and Information Systems (NIS) Directive

The NIS Directive aims to raise levels of the overall security and resilience of network and information systems across the EU. It applies to companies and organisations identified as operators of essential services (OES). The regulatory responsibilities are carried out by Competent Authorities (CAs). The criteria for identifying OES and the list of CAs in the UK can be found within the NIS Regulations.

The NCSC is providing technical support and guidance to other government departments, Devolved Adminstrations, CAs and OES through:

- a set of cyber security principles for securing essential services
- a collection of supporting guidance
- a Cyber Assessment Framework (CAF) incorporating indicators of good practice
- implementation guidance and support to CAs to enable them to:
    - adapt the NCSC NIS principles for use in their sectors
    - plan and undertake assessments using the CAF and interpret the results

What is the NCSC's role in regulation?

The NCSC is not a regulator. However, as the UK technical authority for cyber security, the NCSC provides support and advice to companies and regulators to help minimise the risk of incidents and respond to them effectively if/when they do occur. The NCSC looks to ensure that any requirements are in line with best practice, and that frameworks are consistent across different pieces of regulation.

The NCSC also has a role to provide support during significant incidents, and these incidents may fall under specific regulation. We will encourage victims to consider their regulatory obligations, but recognise that any regulatory reporting or co-operation must be led by the victim.

It is also important to recognise that cyber security is only one aspect of security and business practice, and so there is wider regulation (such as Foreign Direct Investment, or EU restrictions on offshoring data) that must be considered in cyber security decisions.

Appendix 2: Help with cyber incidents

During an incident:

- If you are reporting fraud or cyber crime, please refer to the Action Fraud website.
- If you have been subject to a personal data breach that is required to be reported under the GDPR, please contact the ICO (Information Commissioner's Office). If there is malicious cyber activity related to this which you wish to report (either for information or for action), please complete an the NCSC Incident Form.
- If you are an Operator of Essential Services (OES) under the NIS Directive, please complete an NCSC Incident Form in addition to reporting to your Competent Authority (CA). This is applicable for any cyber incident which you feel requires NCSC's support (for action) or is for wider interest (for information).

Note that depending on the size of your organisation and the nature of the incident, you may receive support from the NCSC, the National Crime Agency or your Regional Organised Crime Units (ROCU).

For ongoing support and guidance:

The NCSC publishes all of its guidance on www.ncsc.gov.uk, and the NCSC twitter feed and LinkedIn page are good ways to keep up to date with new publications. If you want to receive more targeted information and a higher classification of threat intelligence, you should join an industry group in CISP.

Appendix 3: About the NCSC

The NCSC was set up to help protect our critical services from cyber attacks, manage major incidents, and improve the underlying security of the UK internet through technological improvement and advice to citizens and organisations. Our vision is to help make the UK the safest place to live and do business online.

The NCSC supports the most critical organisations in the UK, the wider public sector, industry, SMEs, homes and families. When incidents do occur, we provide effective incident response to minimise harm to the UK, help with recovery, and learn lessons for the future.

The NCSC is the UK government's technical authority and therefore takes the lead role in providing guidance and advice on cyber security for UK organisations. We may also work with Law Enforcement when resolving or investigating an incident, or be asked to contribute to discussions on cyber security policy by government departments such as Cabinet Office or DCMS.

National Cyber Security Centre
a part of GCHQ

Cyber Security Toolkit for Boards

Cyber Security Toolkit for Boards: April 2019 **NCSC_CSTFB_G_02**