National Cyber Security Centre
a part of GCHQ

Cyber Security Toolkit for Boards

Resources designed to help board members govern cyber risk more effectively.

Contents

Foreword

Lindy Cameron - Chief Executive Officer, NCSC

I am delighted to announce the launch of the NCSC's refreshed cyber security Board Toolkit. The feedback we received from non-executive directors and our i100 industry team will ensure the toolkit remains up-to-date, relevant, and framed in language that boards are familiar with.

The vast majority of organisations in the UK rely on information, data and digital technology to function. For businesses today, cyber security is therefore essential, and Board members have a pivotal role in improving their organisation's cyber resilience and exploiting the opportunities that technology brings.

The toolkit helps boards to ensure that cyber resilience and risk management are embedded throughout your organisation. It will help you to make *informed* cyber decisions that are aligned to your wider organisational risks, and ensure cyber security is assigned appropriate investment against other competing business demands.

As a board member it is important to view cyber resilience strategically. Cyber security risk should have the same prominence as financial or legal risks in board discussions. Crucially, cyber security is not just 'good IT'; it underpins operational resilience and when done well, enables your organisation's digital activity to flourish.

The toolkit helps organisations to adopt a methodical and proactive approach to cyber security, and outlines basic safeguards that can greatly reduce the likelihood - and impact - of cyber attacks. I'd encourage all board members to take time to read the toolkit, and use it drive productive cyber security discussions between boards and key stakeholders in your organisation.

Lindy Cameron - Chief Executive Officer, NCSC

Cyber Security Toolkit for Boards

Resources designed to help board members govern cyber risk more effectively.

The vast majority of organisations in the UK rely on information, data and digital technology to function. Cyber security ensures organisations can operate effectively in our increasingly online world.

When it's done well, cyber security is so much more than a compliance function or the implementation of technical controls. You can use it to exploit the opportunities that technology brings, drive your company's agenda, and deliver real value throughout your organisation.

Crucially, good cyber security facilitates better cyber *resilience*; the ability of an organisation to protect itself from, respond to, and recover from a cyber attack, data breach or service outage. The Executive Team, Audit Committee, Risk Committee and Remuneration Committee all have roles to play in making sure that there is the right level of assurance in the business, but **ultimate accountability to the shareholders** is with the **board**.

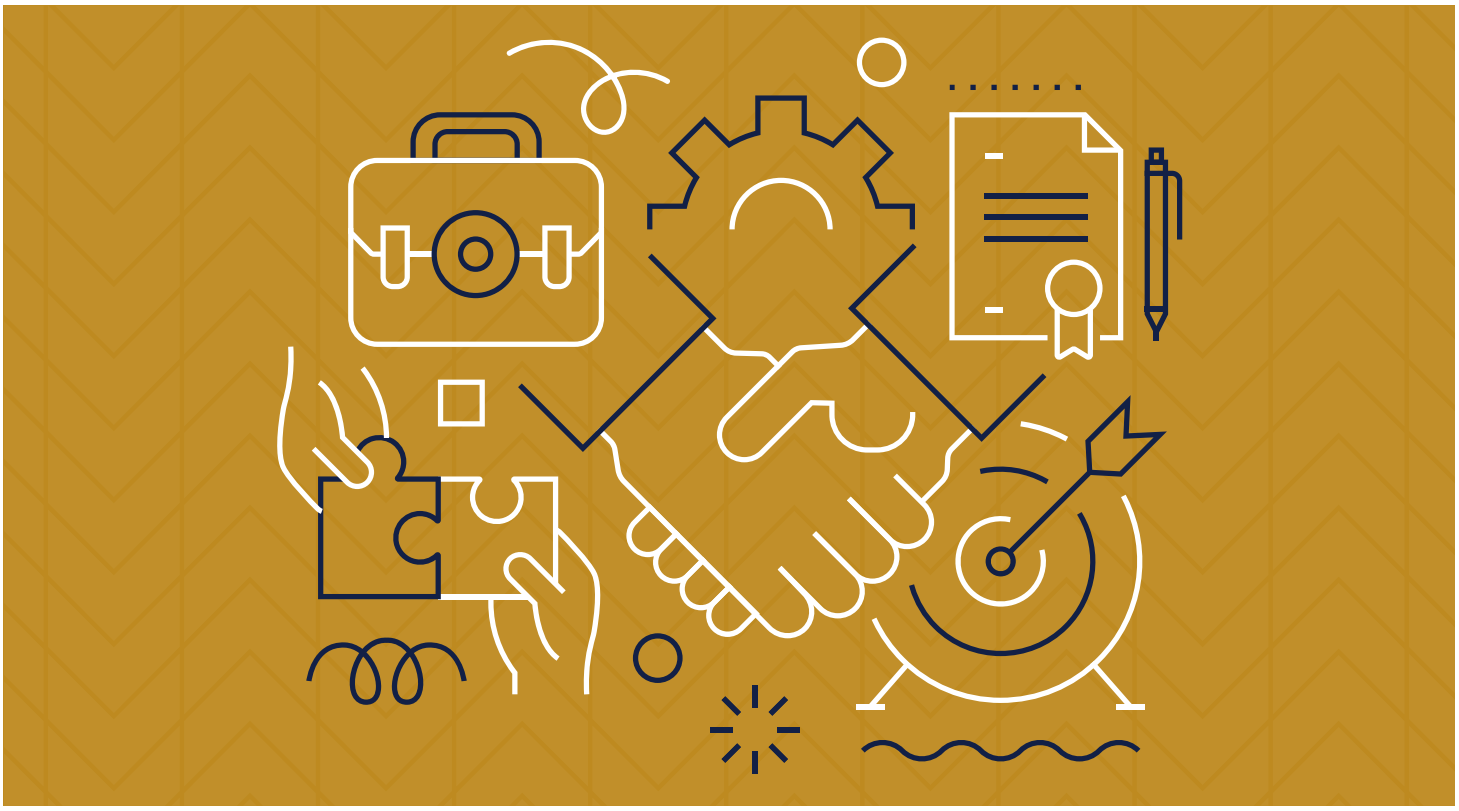
What is the Board Toolkit?

The NCSC's Board Toolkit helps boards to ensure that cyber resilience and risk management are embedded throughout an organisation, including its people, systems, processes and technologies.

What are benefits of using the Board Toolkit?

Boards are pivotal in improving the cyber security of their organisations. The benefits of effective cyber security include:

- Organisations can prioritise areas for investment that balance the value of protection against the needs of the business. This will enable them to create a roadmap for improvements and set aside a budget for the risk exposure.
- Taking cyber security seriously builds trust and confidence with customers and shareholders, particularly at a time where risks and threats are becoming increasingly complex in customer supply chains.
- Organisations that need to demonstrate compliance to regulators are able to do so more efficiently where cyber security is well integrated into the business.
- Organisations that understand their 'enterprise estate' (that is, their people, systems, processes and technology) are better able to identify areas that are critical to the business operation and identify appropriate resources to mitigate against identified threats.
- Organisations with a healthy security culture are able to learn from incidents, driving improvement and innovation. As well as benefits to productivity it can also lead to greater employee wellbeing and retention.
- Investing resources in cyber security training and education enables organisations to prepare their workforce for adverse events and incidents by empowering their decision making.



Who is the Board Toolkit for?

The toolkit is aimed at board members in medium to large organisations in any sector. That could be:

- a Board of Directors
- a Board of Governors/Advisors
- Non-executive Directors or a Board of Trustees

Additionally, committees reporting to the board and security practitioners may find the **Essential activities** section useful in ensuring the organisation is adopting best practices. The included questions will help frame discussions with the board and key stakeholders.

- If your organisation already has a risk management process in place, this toolkit can help you to embed cyber risks through this process, which includes understanding your organisation's overall cyber security strength and resilience.
- If your organisation has a mature cyber risk management process in place, the toolkit will give board members the confidence to challenge how frameworks (such as NIST, ISO/IEC 27005 or CAF) are helping the organisation to achieve its broader objectives.

Regardless of how established your cyber risk process is, the accountability for cyber risk is still with the board, even when cyber aspects are outsourced. Good cyber security has to work for your organisation. 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. Which is why ultimately, cyber security is a board-level responsibility.

Note:

Smaller organisations who may not have the resources to implement the Board Toolkit in full (but still want to improve their cyber security) should, in the first instance, refer to the NCSC's Small Business Guide.

How is the Board Toolkit organised?

Managing cyber security risk is a continuous, iterative process. It can be divided into **3** main sections, and we've organised the toolkit to address key cyber security themes in each one.

1 Create the right enviroment

Organisations should **create the right environment** so that cyber security can flourish by:

- Embedding cyber security in your organisation
- Developing a positive cyber security culture
- Growing cyber security expertise

2 Get the right information to support decision making

They then need to **get the right information** to support decision making, by:

- Identifying the critical assets in your organisation
- Understanding the cyber security threat
- Use this information to evaluate and prioritise risks

3 Take steps to manage those risks

This allows them to **take steps to manage those risks**, by:

- Implementing effective cyber security measures
- Collaborating with your supply chain and partners
- Planning your response to cyber incidents

Note:

This toolkit also also includes an Introduction to Cyber Security for board members who are new to the domain.

How to use the Board Toolkit

In each of the themes above, we've included:

- A summary of the theme that explains what it is, and why it's important
- **Essential activities** that should take place (effectively, the good practices that boards should expect to see in your organisation)
- **Indicators of success:** a series of questions (with possible answers) that boards can use to help evaluate your organisations performance

Note:

The Indicators of success are designed to encourage *productive* cyber security discussions between boards and key stakeholders in your organisation (such as your legal, procurement and HR as well as technical teams). They are designed as a 'starting point', rather than a checklist that's simply to be worked through.

Board members **don't** need to be technical experts, but you do need to **know enough** about cyber security to discuss issues with key staff. The Board Toolkit supports the board by providing the right questions to ask to gain a good understanding of the cyber risk profile of the organisation.

Introduction to cyber security for board members

Cyber security ensures organisations can operate effectively in our increasingly online world.

What is cyber security?

Cyber security is how individuals and organisations reduce the risk of cyber attack. It's core function is to protect the **devices** we all use and the **services** we access - both online and at work - from theft or damage. It's also about protecting the vast amounts of data we access from cyber attacks or compromise, which could disrupt businesses and cause financial loss or reputational damage.

As a Board Member, it's important to view cyber security **strategically**. Cyber security is crucial to safeguarding your operational resilience to ensure that your business can continue to function during an incident. When it's done well, cyber security can be an *enabler* of positive change within your organisation, rather than simply being the *reaction* to a breach. For example, organisations with a **pro-active** approach to cyber security were able to quickly pivot to adapt to the challenge of providing secure homeworking in response to the COVID-19 pandemic.

Cyber security and cyber resilience both have an equal part to play in reducing the cyber risk to organisations:

- **cyber security** focuses on preventing hackers penetrating your IT systems[1]
- **cyber resilience** is the ability of an organisation to protect itself from, detect, respond to and recover from a cyber attack

Taking a methodical and proactive approach to cyber security, and putting in place basic safeguards can **greatly** reduce the risk to your organisation.

1 Organisations that have cyber-physical systems will also need to consider Operational Technology (OT) / Industrial Control Systems (ICS) security and resilience.

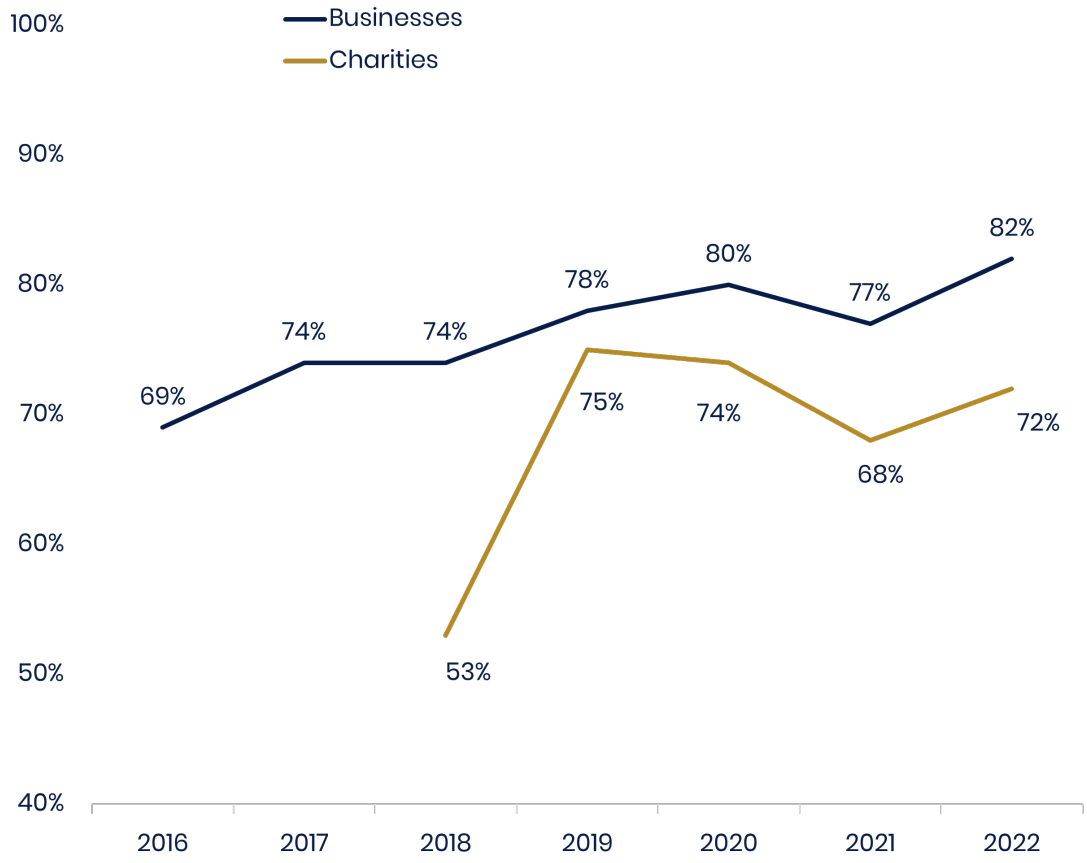
Your responsibility as a board member

The Board is responsible for ensuring that risks to delivering the strategy are identified, evaluated, and mitigated in line with the business risk appetite. This includes:

- understanding the risk that *cyber* incidents present to delivery of the business strategy
- ensuring that the business has adequate cyber resilience to prevent, detect and respond to cyber attacks

Board members **don't** need to be technical experts, but you do need to **know enough** about cyber security to have constructive discussions with key staff, so you can be confident that cyber risk is being appropriately managed.

Encouragingly, the 2022 Cyber Breaches Survey notes that cyber security is rightly seen as high priority for directors, trustees and other senior managers. However, it also notes that "*There is a lack of understanding of what constitutes effective cyber risk management, which is compounded by a lack of expertise and perceived complexity of cyber security matters at board level*".



Percentage of organisations over time where cyber security is seen as a high priority for directors, trustees and other senior managers (Source 2022 Cyber Breaches Survey).

Board members can ensure that cyber security is given appropriate investment against other competing business demands. The Board should rely on its cyber security experts to provide insight, so that the board can make informed decisions about cyber security, aligned to business risks. A senior leader with good understanding of cyber security can improve the knowledge of other board members, increase awareness amongst the wider body of staff, and make the business case for more targeted cyber security spending.

As a board member, you may be targeted

Senior executives or board members are an attractive target for cyber criminals because of their access to valuable assets (usually money and information). Attackers may try and directly target your IT accounts, or they may try and impersonate you by using an email address that appears the same as your own. These attacks work by exploiting the reluctance of staff to challenge requests from someone senior in the organisation. Security policies that are fit for purpose, a positive cyber security culture and well-understood reporting processes will all help to mitigate this risk. You should also consider how personal information about you that is available online (known as your 'digital footprint') could assist an attacker who is trying to impersonate you.

Cyber security: what you need to know

The Board Toolkit briefing packs are an excellent way to introduce cyber security to board members. They are written for a non-technical audience and include slides and presenter's notes for those who wish to deliver the presentations themselves. You can download the presentations and read them in your own time, or watch the NCSC's videos that talk you through the content.

Video: An introduction to cyber security for board members.

Why is your organisation at risk?

It's important to realise that **any organisation** relying on digital technology is at risk of a cyber incident. The majority of cyber attacks are untargeted and opportunistic in nature. Cyber criminals will attempt to exploit a weakness (or vulnerability) in a system, without any regard for who that system belongs to, or the size of the organisation. This means cyber risks need to be **proactively** identified and mitigated. For example, the WannaCry ransomware attack in 2017 was largely possible because software was not being kept up to date, as the following video demonstrates.

Video: The threat from untargeted attacks.

This trend of untargeted attacks is unlikely to change because every organisation - including yours - has something of value to an attacker. It is not just the money you might be asked to pay in a ransomware attack to recover your data. It's also the cost of service disruption, lost business, the damage to your reputation and the cost of investigating and recovering from the attack.

Who is behind cyber attacks?

Despite how they are frequently described, most cyber breaches are **not** a result of 'complex and sophisticated attacks'. The vast majority of attacks are still based upon well-known techniques (such as phishing emails) which can be defended against. The video below summarises the people and groups behind cyber attacks, their capabilities and their motivations.

Video: Who might attack your organisation?

Whilst it's true that *some* attacks are highly sophisticated, these are usually conducted by hostile foreign states who have the money (and motivation) to fund them.

1. Embedding cyber security into your organisation

Cyber security is a team sport: empower everyone

Cyber security is not just 'good IT'; it underpins operational resilience and when done well, enables your organisation's digital activity to flourish. Done well, it can and does add value. This requires a positive cyber security culture and having the right processes in place across the organisation to manage it.

Cyber security impacts **every aspect** of your organisation and it's important for the board to have a clear and effective cyber strategy as part of their business strategy to help reduce risk, financial impact and reputational damage to the organisation. Implemented well, it covers the entire lifecycle from planning, detecting , responding and recovering from a cyber attack. To manage it properly, it must therefore be integrated into organisational risk management and decision making, and all the business units in your organisation should be clear about their cyber security obligations and responsibilities.

For example:

- **Technical teams** need to understand the importance of securing and protecting data and systems through appropriate controls.
- **Human resources** must ensure that cyber security is covered throughout the staff lifecycle, with appropriate guidelines, policy and support for the workforce.
- **Communications and marketing** teams that manage data and marketing services must work with the board to prepare for communications with customers and press so they're prepared for a range of incidents (such as the loss of operational abilities, or data breach).
- **Legal teams** should be aware of the importance of handling and protecting contracts and legal documents to ensure they don't fall into competitors' hands, and need to assure liability risks arising out of potential cyber incidents during operations.
- **Cyber security teams** must design and implement policies that protect employee and customer data from unauthorised access.
- **Procurement teams** need to consider cyber risk when negotiating with potential suppliers of services, from software and hardware to hiring a contractor, and include cyber risk governance within contract management of the supply chain.

Across all business units the workforce needs to be resourced and empowered to implement good cyber security measures. The board should recognise the need not only to protect company knowledge from third parties, but also to co-ordinate and prepare for future incidents.

Essential activities

Governance

It's important that cyber security is integrated into your organisation-wide governance frameworks' including your strategy, risk management processes and compliance and audit procedures. This integration will ensure that cyber security implications are considered in strategic decision making.

The board must understand the cyber risks your organisation needs to manage. Use an independent company to carry out a cyber risk assessment to provide an informed overview of your organisation's cyber security posture and data for effective decision making.

Cyber governance also includes policies, procedures, roles, responsibilities, organisational structure and controls to protect your organisation from cyber threats. You'll need to determine how effective your current cyber risk governance is and identify gaps and areas to build upon.

The following non-exhaustive list of frameworks can help with this process:

- Cyber Essentials is an effective, government backed scheme that will help you to protect your organisation, whatever its size, against a whole range of the most common cyber attacks.
- For larger organisations, ISO/IEC 27001 is an internationally recognised standard for the establishment and certification of an Information Security Management System (ISMS). It is important that the scope of the system certified is broad enough and reflects an organisations operations. For CNI and other regulated sectors, additional frameworks may also be appropriate, particularly those that have OT (operational technology) in addition to IT.
- The NCSC Cyber Assessment Framework (CAF) helps organisations that play a vital role in the day-to-day life of the UK (such as those designated as forming part of the critical national infrastructure, or subject to certain types of cyber regulation) to achieve and demonstrate an appropriate level of cyber resilience.

The Introduction to security governance pages provide helpful guidance for evaluating whether the framework you are using is appropriate to your context. In addition, Exercise in a Box is a free online tool from the NCSC which helps organisations find out how resilient they are to cyber attacks, and to practise their response in a safe environment.

Effective communication

Improving the communication between business units and the board requires effort from both sides, as well as a readiness to acknowledge each other's priorities. Boards need a 'good enough' understanding of cyber security to appreciate how it supports their overall organisational objectives. Business units (with their understanding of what is happening at an *operational* level) must have the opportunity to flag the issues and recommend actions to the board, while understanding the board's concerns for operational and reputational risk.

Charity use case

WaterAid's Cyber Security and Vendor Manager, Mark, explained how the NCSC's Board Toolkit has been useful for their organisation and stated, 'Our board of directors is made up of CEO's from other organisations and the board toolkit has been key in driving the cyber strategy and engaging other parts of the organisation. Following the board toolkit proved to be a real enabler for us in receiving support from key stakeholders and has really strengthened our thinking.'

Natasha, their senior internal auditor, added, '*Yes, as very much a non-IT person I found it an incredibly helpful framework for designing a high-level internal audit review of our cyber security arrangements. I used the toolkit's questions for board members and management as the basis of the audit working paper. Going through these questions with a member of our board and colleagues from IT and other teams helped me develop a better understanding of where our cyber security is strong and where there might be risks which we had not previously considered. The audit delivered a number of recommendations which management is now actioning to make improvements.*'

Indicators of success

Has an independent cyber security risk assessment been carried out?

This is key to understanding the cyber risks your organisation needs to manage, and the organisation's security posture. The result of the assessment will provide the board with an independent view of the organisation's cyber resilience, enabling effective decision-making which will inform the cyber strategy.

Is a cyber strategy in place?

A cyber strategy that supports your business strategy helps your business to reduce risk, financial impact and reputational harm. This is a plan of **high-level actions** to improve the resilience in your organisation and should cover your highest priority critical concerns (for example, unpatched software or obsolete devices). It should also include:

- planning your response to an incident
- exercising incident response procedures
- detecting, responding to and recovering from a cyber attack
- employee cyber awareness training

The board should receive management information on how the cyber strategy and plan are being delivered, and this should be reviewed at least annually or in line with current threat level.

Does cyber security feature in the priorities of all business units across the organisation?

A good indicator that cyber security is embedded into your organistion is if *all* business functions (such as HR, legal, and public relations) are working collaboratively on cyber security initiatives. If cyber security is being left entirely to technical teams, this is a sign further alignment and investment is required.

Does everyone know where accountability and responsibility sits?

Accountability and responsibility for cyber security should be clearly defined. If senior leadership and/or members of the board struggle to clearly and consistently identify where responsibility and accountability sits, this is a sign that work needs to be done on reporting structures or on the communication and visibility of reporting structures.

Do all Board members get involved in discussions of cyber security?

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 online sales, contractual relationships, your reputation, 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.

Do cyber security reports help support decision making?

Key Performance Indicator (KPI) dashboards simplify the reporting process and provide the board with clear and up to date information to support good decision making. You should expect to see KPIs with an agreed target range for each measurement on what's acceptable These might include the time taken to implement security patches and mitigate high risk vulnerabilities, and the number of days between detection and remediation.

2. Developing a positive cyber security culture

People are the strongest link; they're what make your organisation thrive.

Security culture refers to the values that determine how people are expected to think about and approach security in an organisation. These are shaped by the goals, structure, policies, processes, and leadership of your organisation.

A positive cyber security culture is essential because it's **people** that make an organisation secure, not just technology and processes. If this is in place, people view security as a collective and collaborative endeavour that supports and is supported by their everyday work.

If there's a good security culture:

- employees are more likely to spot problems and suggest potential improvements, which leads to greater resilience
- employees can communicate openly about issues without fear of reprisals, and are much less likely to make use of shadow IT services
- you'll improve employee wellbeing and retention, driven by inclusivity and an understanding of *why* security rules exist

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

Developing the right culture is a continuous process. It takes time, investment, and buy-in from senior leadership. *You can* encourage behaviours that create the right cyber security culture. You *can't* simply 'change' a culture to create the right behaviours around cyber security. Culture is an outcome, rather than an input.

Essential activities

Leadership

There must be strong cyber security **leadership** that is communicated and championed by the board. Board members set the tone when it comes to cyber security culture. If senior leaders ignore policies and processes, or ask for special treatment in some way, this tells everyone else in the organisation that it is acceptable to try to bypass them.

Clear communication

Ensure your cyber policies are developed in collaboration with the workforce and that they are **clearly communicated** so that everyone in your organisation can understand the risks, their responsibilities and what actions they need to take if required. Your senior leadership should be communicating clearly about cyber risks and policies (for example, through 'town hall' meetings, in-house communications and team meetings). The Board should **not** be working solely in a top-down fashion; they should be listening carefully to people from across the organisation and understand how changes impact the way in which they engage with cyber security.

Simple reporting for incidents

Whilst technical monitoring can look for anomalies, people can act as an early-warning system and intuitively spot something that looks unusual. Ensuring there is a simple process in place for employees to report incidents (where they feel comfortable reporting concerns) can save the organisation a huge amount of time and money. If staff are working around a set procedure, this may highlight a particular policy or process that needs to be addressed . Work with your policy makers to adapt it. The following video below provides common examples of how staff working around security policies can highlight problems with security policies.

Video: NCSC CYBERUK 2017

Your organisation's cyber resilience approach should include a strategy for learning from incidents, and what went well, so that your security posture improves over time. Treat incidents as a learning opportunity so that individuals can reflect openly on what happened and feel confident to speak up and report concerns. Put in place processes to capture this information.

Training

Your organisation should have a **cyber security training programme**. Programmes should be evaluated and (where necessary) improved on a regular basis. Consider rewarding people for demonstrating good cyber behaviours.

Indicators of success

As a board member, do you lead by example?

Board members should be good role models when it comes to cyber security behaviours. This includes keeping the data and information you use safe and secure, and knowing what to do if you feel you have been targeted. Speaking openly and positively to employees about why cyber security is important to the organisation will improve the cyber security culture within your organisation.

Can you demonstrate a collaborative approach to security policy and process design?

Cyber security is a shared responsibility. If your organisation is developing a positive cyber security culture, it should be possible for your security team to demonstrate how security policies and processes have been designed in collaboration with HR and training teams to really address the problem and improve the culture. If it is hard to point to ways in which policy or process has been shaped by the wider organisation (including business process owners), this may indicate a less mature cyber security culture.

Do you have a 'no blame' culture?

No blame doesn't mean no accountability. Learning from incidents is key to understanding why something happened and preventing it in the future. For organisations with a positive culture, incident reports provide an opportunity to reflect on what could have been done differently, including the root cause, the actual response and how the organisation could improve. If the report focuses on individuals or teams who are 'behind the problem', this is a sign that you have a less mature cyber security culture.

Do your security metrics focus on success rather than failure?

Metrics express the organisation's values, and if you appear to value the absence of reports of problems, you incentivise people to keep quiet about issues. Consider how you can formulate your security metrics in terms of successes. For example, as well as measuring how many people clicked on a phishing email, focus on how many people reported it.

3. Growing cyber security expertise

As the demand for cyber security professionals grows, your organisation should plan ahead to draw upon expertise.

Cyber security covers a broad range of disciplines. Senior Leaders should ensure that recruitment and training meet their cyber security needs. This can be challenging as technologies, threats, and organisations constantly change. You'll need a dynamic approach that aligns business objectives with the cyber security needs of the wider organisation.

The benefits of growing your cyber security expertise include:

- organisations that retain cyber expertise within their workforce have a competitive advantage
- an established and experienced workforce can more effectively manage cyber resilience and empower employees
- recruiting a diverse workforce will ensure your organisation has the diversity of thought necessary to tackle demanding cyber security challenges
- training helps organisations remain compliant with laws and regulations

Essential activities

The most effective approach will depend on your context, but may include a combination of investing in your people, bringing in external experts or companies, and developing a pipeline of talent. The assessment of cyber skills might be an activity within the overall people/talent-planning part of the business, and the board should have sight of this.

Workforce training

Implementing expertise and workforce training will need input from people across the organisation, including your HR, IT and finance teams. Your training provision should be reviewed regularly to account for changes in the cyber landscape and business needs. Note that 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. The NCSC Certified Training scheme is designed to assure high quality cyber security training courses.

Baseline your expertise

Your organisation's needs for cyber expertise should inform recruitment, derived from a **baseline of your organisation's current cyber expertise**. It should identify key gaps and areas of weakness, and set out the approach and urgency to address these issues. Buying in expertise where required can provide a quick solution where there's a lack of specialised cyber security knowledge.

You might want to consider:

- recruiting a skilled non-executive director to your board
- employing a consultant to provide specific cyber security advice (a good place to look for external expertise is NCSC's certified cyber professionals)
- identifying specific cyber security services which can be fulfilled by a third party
- making use of established, commodity technologies, which frees your own experts to spend time exploiting the unique insight they have into your organisation (for example, you might choose to allow cloud vendors to build and secure your infrastructure)

Cyber awareness

Your organisation must have an overarching cyber awareness programme which includes a basic level of cyber security awareness for all employees to be carried out at least annually. If you don't have any existing programmes, the NCSC'S online training package, 'Top Tips for Staff' can be used as a starting point, and is provided in a format so that it can be built into your training resources.

You should also consider using outside speakers, awareness posters and company wide messaging for disseminating new insights and guidance to appropriate parts of the business. These may come from the NCSC, or from participation in sector-wide forums, and events like CYBERUK. These initiatives should be co-designed with employees, including comms and training teams, and should be run at all levels from the board down. Leadership play a key role in the success of the programme through effective communication and securing organisation buy-in.

Talent pipeline

Develop future staff through 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. 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. Ensure that your cyber strategy includes components on cyber expertise, cyber development plans and staff training. It will need input from people across the organisation, including HR, IT , and finance teams.

Indicators of success

Can your HR team point to specific cyber skills areas which are currently needed by the organisation, and is there a plan to address the gaps?

Whoever reports to the board on HR matters should be able to report on the specific skills gaps that the organisation is facing at that time with a plan in place to develop cyber expertise where required. The board should be supporting this both in terms of investment and broader resources.

Are you seeing improvements in metrics of cyber hygiene?

These might include levels of user engagement in phishing emails (exercise and real), levels of incident reporting by staff and scores in awareness training.

Do you have good employee retention in key cyber security roles?

Problems with retention of staff may serve as a signal of broader systemic issues that need to be examined.

Does the diversity of your staff compare favourably with business and industry-reported figures?

If it does not, then your organisation might not be drawing and nurturing talent from the largest possible pool, which will put your organisation at a competitive disadvantage. Equality, diversity and inclusion should be integrated throughout (a good set of starting points are recommended in the Decrypting Diversity report).

Does your organisation review cyber skills to establish gaps on a regular basis?

What counts as 'regular enough' will depend on your context, but if the document is not reviewed at least annually, this indicates that your approach to skills and expertise may no longer be aligned with the organisation's current conditions.

Does the board have sufficient knowledge to make strategic decisions about cyber security?

Cyber criminals are quick to exploit new and emerging technologies. As the threat landscape evolves, it is important to regularly assess whether the board would benefit from additional specialist support to ensure you are equipped with the knowledge to provide rigorous oversight of the organisation's cyber resilience.

4. Identifying the critical assets in your organisation

Understanding how technical assets are critical to your organisation's objectives is key to effective risk management.

Effective cyber security risk management depends upon your organisation:

- having a good understanding of its technical estate (the various systems, data, services and networks that are used by the organisation)
- being able to identify which are the critical assets upon which your key business objectives depend

The board will therefore need to communicate key objectives (one 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.

Understanding your technical estate is important because:

- it helps to mitigate cyber security risks (for example, if you're not aware of the entirety of your technical estate during a malware attack, forgotten systems may re-infect the estate when the system is brought back up)
- knowing which systems are connected (their dependencies, who has access, and who manages which component) are all critical to setting good defences and recovering from cyber incidents
- many incidents are the result of vulnerabilities in acquisitions, or in older legacy systems that **can** be defended against; these are often low-value assets that are overlooked
- by documenting each IT asset and its critical dependencies, IT teams gain greater insight into the security controls needed to meet business, legal and regulatory requirements

This may seem like a daunting task, especially for organisations whose networks and systems have grown organically, but even a basic understanding of your estate will help. Identifying the critical assets can give you a starting point, from which you can identify dependencies.

Note:

Some organisations will also need to consider controls on their Operational Technology (OT) systems (which can be complex due to the intricacies of legacy assets, or even be spread over multiple sites).

Essential activities

Work out where you're starting from

Ensuring your organisation understands its assets (such as including hardware, software, peripheral devices and removeable media) is a precursor to being able to address the resulting risks. Records should include who is responsible for each asset, where it is stored and what it is used for. This can help you identify critical technology assets and where vulnerabilities may exist in your environment. It should also include those belonging to any third parties which your organisation depends (for instance Software as a Service providers or cloud hosted applications) that are crucial for day-to-day operation. Ideally, your inventory should also include a set of reference architectures for all the systems you depend on.

Maintain a comprehensive inventory

Larger organisations with complex estates may want to invest in an IT asset management solution to help you do this, for both physical and virtual assets. Your approach will need to adapt to conditions, for instance company acquisitions and mergers can create additional complexity.

Prioritise mission critical activities

The board should take a holistic approach when considering what is critical to the organisation. For example, the board might know that a specific partner is vital, 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' (ie 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

Collaborate with other teams

Identifying critical assets upon which your core objectives depend cannot be done by your technical team alone. It requires strong collaboration between business and technology functions, and a thorough understanding of the assets themselves as well as the core business objectives. Your baseline and understanding of critical assets should be cross referenced by other key strategic plans, such as your business continuity plan, or plans for remediation of legacy systems. For organisations with cyber-physical estates, it will require the collaboration of operational technology teams. It should not **just** be an inventory 'by your IT team of those assets under their control', but should span the entire organisation, and your wider supply chain where necessary.

Indicators of success

How complete and up to date is your inventory?

If sample checks on the accuracy of the asset inventory are carried out monthly and MI is shared with the board, any gaps will be identified. Independent audits should also take place to ensure the data is accurate and up to date.

Do you have assurance that changes are considered and recorded to keep the baseline up to date?

This is essential in mitigating potential risks that any undocumented systems might pose.

Does the board have assurance that the critical assets are known, who is responsible for each asset, what it is used for and where it is stored?

This information is essential to ensure that measures are in place to protect those assets from being compromised. Some information assets will have to be protected in line with regulations and laws and the board needs to be aware of these and have assurance that the systems and processes that the regulations may require are being met.

Have the priority objectives been clearly communicated and is there assurance that those priorities guide cyber security efforts?

If your critical assets can each be cross referenced to a clearly stated core business objective, this is a sign that your organisation is taking the right approach. For example, if a promise to customers about their privacy is a priority then you might identify what could jeopardise this promise (eg the loss of their credit card details) and what technical assets are required to secure those details (ie an access management system) ? This would allow you to prioritise defending these assets when implementing cyber security measures.

5. Understanding the cyber security threat

Threat intelligence is key for organisations looking to build cyber resilience.

Understanding the threats faced by your organisation will enable you to tailor your organisation's approach to cyber security investment accordingly. You need to prioritise what threats you are trying to defend against, otherwise you risk trying to defend against everything, and doing so ineffectively.

The benefits of building your understanding of the cyber security threat include:

- Organisations that are routinely gathering information from reliable sources (such as the NCSC's threat report) are able to respond rapidly and appropriately to new and emerging threats.
- Knowing how you are exposed to cyber security threats will help your security team to focus their attention on the most important areas, and use your resources as efficiently as possible.
- A thorough understanding of different threats will help an organisation clearly communicate the rationales for security measures to staff, leading to a better degree of compliance.
- Robust risk management as the threats are understood and managed. This can be particularly important during periods of transition, for instance when preparing for a merger with a company which may be exposed to a different level or type of threat.

Essential activities

Understand the cyber security threat landscape

The board should have an awareness of the wider threat landscape through a regular threat briefing. This should include current threats which could affect all organisations and those that are specific to the business. Changes in the threat position should be included in the management information that the board receives at its board meeting. Sign up to the NCSC's threat reports and advisories on cyber security matters affecting the UK.

Build your threat assessment into your risk management

Ensure that your organisation carries out regular threat assessment exercises to identify who might attack your organisation, their capabilities and motivations. This should involve suppliers and partners as many organisations have close dependencies on external parties for critical assets or as part of a supply chain. The outputs of the threat assessment should feed into the risk management process, and unacceptable risks should be escalated to the board.

Consider threat intelligence

You should consider acquiring deeper level of threat intelligence, especially if you're a larger organisation dealing with critical infrastructure. For instance, organisations operating a Security Operations Centre (SOC) will typically make use of finer-grained information, via the NCSC, commercial providers, or open source, about indicators of compromise and the tactics and techniques in use by adversaries.

Collaborate on security

The people responsible for cyber security in your organisation should participate in collaborative information sharing forums with sector peers. Attackers often target a number of organisations in the same sector in a similar manner. The NCSC's Cyber Security Information Sharing Partnership (CISP) 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.

Traffic Light Protocol (TLP)

Collaborating with your competitors may seem counter-intuitive, but there is a precedent and well-established process for sharing information in a way that protects commercially sensitive information, known as the **Traffic Light Protocol (TLP).** It is used to allocate a sensitivity category to information. There are four information sharing levels: RED, AMBER, GREEN and CLEAR.

RED Non-disclosable information, restricted to representatives present at the meeting. Representatives must not further disseminate the information. RED information may be discussed during a meeting, provided all representatives present have signed up to these rules. Guests and others such as visiting speakers who are not full members will be required to leave before such information is discussed.

AMBER Limited disclosure and restricted to members of the forum and those within their organisation (whether direct employees, consultants, contractors or outsourced staff working in the organisation) who have a need to know in order to take action.

GREEN Information can be shared with other organisations, or individuals in the cyber security community, but not published or posted on the internet.

CLEAR Information that is for public, unrestricted dissemination, publication, web posting, or broadcast. Any member may publish the information, subject to copyright.

Note:
Ensuring that collaboration between competitors is continuous is likely to require board-level support.

Indicators of success

Can board members name the top cyber security threats faced by the organisation and outline the measures that are in place to mitigate their impact?

An easy indicator for whether your organisation has clearly articulated the key cyber security threats is whether these issues have been communicated to the board. For instance, for many organisations, ransomware attacks by organised cyber criminal groups are at or near the top of the list. Board members should understand the nature of these threats, how they affect business objectives, and how the organisation is addressing them.

Do threat assessments involve representatives from across the business, and are they linked to your cyber risks?

It can be easy to regard threat assessment as a primarily technical exercise, but in addition to technical knowledge, it requires a close analysis of business objectives to inform prioritisation and assess attacker motivation. If your threat assessments involve stakeholders from across the organisation and cover your highest priority risks, this is a good sign that a well integrated approach is being taken.

Do you have relationships with representatives from other organisations in your sector?

Collaboration is at the heart of good understanding of cyber threats, and if relationships across the sector are established, this is a good sign of wider cyber resilience. For example, if your technical team are making regular contributions to CISP (described above), this is a good sign that they are developing sources of insight and collaborative relationships that will assist them in their threat assessments. If collaboration is limited in your sector, consider how the board may play a role in creating and supporting cross-sector forums.

Are your experts attending key cyber security events?

Events such as CYBERUK, RSA Conference and Black Hat Briefings Conference are examples of events that give key staff the opportunity to ensure they're on top of the most up-to-date developments and cyber threats.

6. Risk management for cyber security

Good risk management will help you to make better, more informed decisions about your cyber security.

Every organisation has to make difficult decisions around how much time and money to spend protecting their technology and services. One of the main goals of cyber risk management is to *inform* and *improve* these decisions.

Cyber security risk management therefore has a huge impact on an organisation's ability to achieve their goals. It helps organisations identify their 'security posture' (that is, their overall status of cyber security readiness), mitigate risks, and ensure that resources and investment are spent in the right areas. It should also *support and enable the business*, and it should do this by managing its risks without slowing things down, or making the cost of doing business disproportionately expensive.

Many of your operational and organisational risks will have a cyber component to them. Cyber *security risk* should therefore be **integrated** within your overall approach to risk management, and **not** be dealt with as a standalone topic (or considered simply in terms of 'IT risk').

Avoiding tick-box compliance

Encouragingly, many organisations are already taking steps to assess and manage their cyber security risk[1]. However, it's worth checking what's driving this activity. Carrying out cyber risk management solely for 'compliance' purposes can lead to risk being managed in a 'tick-box' fashion and can prevent organisations questioning whether they have ticked the right boxes, leading to overconfidence in how well risks have been managed.

While it's important that controls are in place to demonstrate compliance with laws and regulations relevant to your sector, 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; it should give insight into the health of your organisation and identify not just issues, but potential opportunities.

1 Just over half of businesses (54%) have acted in the past 12 months to identify cyber security risks [Source, DCMS Cyber Security Breaches Survey 2022]

Essential activities

Perform risk assessments, and review regularly

You should have assurance that your organisation has chosen a method or framework for managing risk that fits with the organisation's business and technology needs, and changes to risk are assessed at least bi-annually[1]. Some commonly used compliance frameworks that can help with this (including ISO/IEC 27001, NCSC Cyber Assessment Framework and Cyber Essentials) are discussed in the section on Embedding cyber security into your organisation . Setting a risk appetite for cyber will help define the 'level' of risk an organisation will manage when pursuing its objectives, thereby aiding effective decision making.

1 For organisations operating in high risk or regulated sectors who are going through business change, exposed to more sophisticated threats, geo political changes or similar will need to review on a more regular cadence. It will be for senior leadership to discuss and agree this cadence.

Integrate cyber security risks with operational and organisational risks

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 (the most significant being the security implications of 'unmanaged' devices connecting to the organisation's networks). But there are also cost and liability implications. Were these considered 'in the round' when making the decision? Or was security only discussed once the decision was already made?

Reporting from audit/risk committee meetings

The board has a responsibility to ensure that risks to delivering the strategy are identified, evaluated, and mitigated in line with the business risk appetite. Cyber presents a critical risk to most businesses, so it is vital that the committee chair communicates the organisational risks clearly to the board so they understand the risk that cyber incidents present to delivery of the business strategy.

Use risk metrics with caution

Don't make reducing risk levels the measure of success. While risk metrics generated (such as risk numbers, risk levels and impact levels) are useful, they can easily be misinterpreted if used in isolation. It is important that parties collaborate to understand and agree the meaning and context of the risk management information provided.

Stay informed regarding managing risk for newer technologies

You may need to review *cyber security* risks more regularly than other risks. Cyber security is still a relatively new field, so your organisation won't have as intuitive an understanding of *cyber security risks*, as it might for say, *financial risks*. As new technologies emerge, there might not be a huge evidence base to draw on to form a risk assessment. NCSC guidance will help to identify and assess cyber security risks (as we have done for Cloud Security).

Indicators of success

Do we know the current risks the business is exposed to from cyber events?

This is difficult to capture when every industry sector will have different priorities based on their size, sector, and risk appetite. It might be easier to consider reputational impact, financial loss, operational impact, personal impact, and where these are felt within the organisation. If you are aware how many risks are within the agreed threshold (and the cost of the high priority risks that are outside it), that would be a good indication that the board has a good understanding of cyber risk.

Do we have a process that ensures cyber risk is integrated with business risk?

In assessing all key risks, a key question for the board to ask is 'Have we considered cyber security risk in the decisions we make'? For example, a company that is bidding for a contract will have lots of risks associated with pricing, quality and competitors, but there is also a cyber risk (namely, it's possible that commercially sensitive bid information is stolen by a competitor or an insider, and the information is then published on the internet).

Do we have an effective approach to manage cyber risks?

The board need assurance that a cyber risk register is in place (as part of the overall organisation risk register), that covers risk ownership and an escalation mechanism for the whole extended enterprise (eg front line business units, subsidiaries, suppliers and partners, and in some cases customers.) This should involve all of the key stakeholders in the organisation and reflect the agreed priorities and tolerances endorsed by the board. It should take account of change (for example business priorities, technology changes and geopolitical or economic context). The NCSC's detailed Risk Management guidance includes advice on choosing suitable frameworks for your organisation.

Has the board clearly set out what types of risks it would be willing to take, and those which are unacceptable?

Be specific when defining what is and isn't accepted. Whilst you might be unwilling to tolerate any significant risk to *personal data*, you might be willing to accept email being unavailable for a day. Also consider the cumulative risk you are accepting; it's possible that all your cyber risk could be realised at the same time and and at a crucial time of the year i.e end of year financial reporting, important retail periods, annual events. 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.

7. Implementing effective cyber security measures

Put in place defences that will protect your critical assets against the biggest threats.

Implementing effective 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. Even basic cyber security controls can reduce your exposure to cyber attacks, and lessen the associated reputational, financial and legal impacts.

With a baseline of cyber security controls in place to mitigate against the most **common** cyber attacks, you should then tailor your defences to mitigate **your organisation's 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. You will need to consider various factors including your organisation's risk appetite, and the sensitivity of the data you hold.

Implemented well, security measures will also help your workforce do their jobs effectively, leading to improvements in productivity and better compliance.

What are security measures?

By security measures, we mean steps that you put in place to mitigate a known cyber security risk. It's important to note that this will be a mixture of both explicit and implicit measures:

- an *explicit* measure is one that uniquely addresses a specific cyber security risk alone; for example, antivirus software is designed to detect, stop and remove viruses and other kinds of malicious software
- an *implicit* measure addresses a cyber security risk, but will also provide value to the business in other ways; for example, an asset management system can help you make good procurement decisions and speed up financial reporting, but it also addresses the cyber security risk of ensuring software is kept up to date (so it's less vulnerable to cyber attacks)

This means cyber security measures won't always be *technical* products or services, but are just as likely to be processes, training or policy. Cyber insurance is **not** a technical measure (so won't defend against a cyber breach or attack), but it can offer some financial security during an incident.

Essential activities

Tailor your defences to your highest priority risks

Your organisation should take a risk-based approach to implementing cyber security measures. Your measures will be tailored to protecting the things you care about the most, against methods used by specific attackers. All measures should be traceable to the specific cyber security risks they mitigate.

Use established security controls

Cyber criminals often use common methods to attack an organisation. A lot of these methods can be mitigated against by implementing well-known cyber security controls. There are several frameworks that outline what good cyber security controls look like. These include the NCSC's 10 Steps to Cyber Security, ISO/IEC 27002 and the Cyber Assessment Framework (CAF).

Layer your defences

As with physical and personnel security, cyber security can make use of multiple measures which (when implemented simultaneously) mitigate single points 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.

Conduct regular reviews of your measures

Cyber attackers adapt and evolve, and your security needs to do likewise so testing the effectiveness of your security controls is important. You can review defensive measures against suitable frameworks such as Cyber Assessment Framework (CAF), or certification schemes such as Cyber Essentials.

You should rehearse how your organisation responds to cyber attacks by using the NCSC's Exercise in a box tool, which provides a safe environment for your organisation to assess its resilience. In addition, it's good to consider testing your organisation systems and security processes by emulating an attacker hacking into secure systems or data by 'red teaming'. A 'red team' can be an externally contracted group of penetration testers or a team within your own organisation, tasked to hack your environment using real world techniques in order to test a wide variety of cyber attacks, breach scenarios or organisation specific risks before they occur.

Defend against someone inside your network

Your cyber security approach should recognise that a criminal (which can range from a disgruntled employee to a state funded individual intent on stealing your intellectual property) will be able to access your system. This means you need to have controls in place to minimise the harm that they can do once they are inside. You can do this by restricting the access they have to service and information. Monitoring and logging are key to being able to detect signs of malicious activity as quickly as possible, and limiting the damage they can do.

Fraud use case

A charity organisation was first aware there was an incident when their bank contacted them querying a change in a suppliers bank details.

Their CISO explained, *'We checked the Finance Manager's email account and discovered that a rule had been set up to divert any email containing the words 'payment', 'invoice', overdue' bank details' etc to the Really Simple Syndication (RSS) feeds folder. At this point the fraudster doctored the body of the email and the invoice attachment with the fraudulent bank details. It was believable as the main body of the email had clearly come from a known supplier as it was answering questions that only they could have known. We thought at this point that we had narrowly missed making a payment to a fraudulent bank account.'*

Another supplier emailed a week later to chase payment of an invoice which the organisation thought they had paid. On checking the payment details they discovered the payee's account details were different to those on the invoice.

'Looking back, the Finance manager had noticed that people were saying that they had sent her an email but they were taking a day or two to come through but it was just thought to be a lag with the system. This will be a red flag alert going forward.'

Immediate Action Taken

- Finance Manager called the bank and alerted them to the fraud
- We reported to Action Fraud in order to obtain a crime reference number
- We reported to The Charity Commission as a serious incident

Lessons learned/further actions

- We updated our processes and procedures
    - weekly checks on email account to ensure no rules have been set
    - check email 'safe senders' list to make sure it is authentic
    - check the location of any logins to Microsoft 365 to ensure no activity on the account
    - check RSS Feed folder for rogue emails
    - bank details for new and updated suppliers to be verified by a phone call
- If making a payment online and bank details don't match, phone and check with the payee that the details are correct
- Implemented multi-factor authentication for logging into Microsoft 365

Indicators of success

Are effective security metrics shared with the board?

These facilitate decision making and improve performance and accountability. They should be aligned to key business functions, and could include mean time to detect and recover from an incident. These metrics provide the board with the information needed to discuss the investments needed to bring about improvements.

Does the board understand the overarching purpose of the cyber security measures?

While there are a lot of technical details involved in assessing threats and risks (and the measures that protect against them) if the overarching approach to determining and reviewing measures can be easily explained and is understood by the board, that is a good sign that an effective approach is being taken.

Can new implementations of cyber security measures be traced to the risks they mitigate?

Ensuring that the focus of your cyber security measures is aligned with the risks you have identified and prioritised is a key indicator that decisions are being taken in light of the actual threats your organisation is facing.

Are new implementations of cyber security measures being rolled out in close engagement with the workforce?

This may include piloting them, co-designing, or testing how well they work. Engagement with the workforce is an important sign that the measures are implemented in a way that is likely to deliver value .

Has your cyber security posture been reviewed in the past 12 months?

The nature and depth of that review may vary, but if an overall review has been conducted in the recent past, that is a good sign that you can continue to be confident that your measures have remained effective.

8. Collaborating with your supply chain and partners

Cyber attacks on your suppliers can be just as damaging as an attack on your own networks.

Many of us rely on suppliers to deliver products, systems, and services. However, supply chains are often large and complex, which makes it difficult to know if you have enough protection in place. Whilst you might be implementing cyber security effectively within your own organisation, you're exposed to numerous risks if your suppliers have not done the same.

In recent years there's been a significant increase in the number of cyber attacks resulting from vulnerabilities within the supply chain. These attacks can result in devastating, expensive and long-term ramifications for affected organisations, their supply chains and their customers (as the following video explains).

Video: NCSC Board Toolkit - NotPetya

Despite these risks, many companies lose sight of their supply chains. According to the DCMS 2022 Security Breaches Survey:

- only 13% of respondents reported reviewing the cyber security of their immediate suppliers
- only 7% went deeper into their supply chains

Board leadership can make an important difference, by encouraging collaborative relationships between organisations and their suppliers. The benefits of doing this include:

- Close collaboration with suppliers and partners can greatly enhance your cyber security, is likely to reduce the chances of a damaging cyber attack, reduce your overall risk exposure, and improve your response time and ability to manage the impacts of cyber attacks should one occur.
- Understanding the cyber security of partners is essential if you are to gain assurance that threats from the supply chain are understood, and risks mitigated (the NCSC has published guidance that helps you do exactly this)
- Where you are part of other organisations' supply chains, your ability to convey your own cyber security approach can be a driver of new business opportunities. Being able to demonstrate a good level of cyber security is increasingly a key component of supplier and provider bids, and is already a requirement for many government contracts.

The overarching goal of a supply chain cyber security assessment is to gain assurance about the cyber security of suppliers and partners, and their services and products. This should be **in proportion to the level of risk**, rather than expecting all suppliers and partners to be at the same level of maturity. In some cases, risks can be minimised with simple measures. In others (for instance where you are installing cyber security solutions which will have comprehensive access to your digital assets) you may need to seek extensive assurance from your suppliers that you will not be exposed to risks through them.

Essential activities

Map your suppliers

Building a clear picture of your suppliers (and working with them to establish *their* subcontractors) is imperative to supply chain security. You should have assurance that your organisation has a process in place for assessing suppliers, understanding the nature of your dependencies on them, the maturity of their cyber security posture, and steps to be taken to address issues.

Communicate across multiple links

Look for opportunities to enhance resilience and raise awareness by requesting that your suppliers expect similar standards from their own subcontractors or suppliers. If your customers are failing to communicate their own security needs to you, challenge them to be explicit and to provide assurance that they are happy with your arrangements.

Build cyber security into contracts and agreements

Ensure compliance with minimum cyber security requirements is mandated in your supplier contracts and ask for evidence that controls are in place. Ensure security practices are embedded throughout the contract lifecycle of new suppliers, from procurement and supplier selection through to contract closure. Your contracts should include details of what will happen in the event of an incident. If you depend upon a supplier for information about an incident, you may need to specify timelines and onward reporting responsibilities to ensure compliance with legal and regulatory requirements.

Use threat intelligence

Develop threat assessments, threat modelling and rehearsals of incident response with key suppliers and partners. Consider scenarios affecting multiple organisations and/or systems. Analyse how a breach or outage at one organisation could impact the operations of another. Joint exercises can have mutual benefits in building understanding of shared risks, as well as in sharing expertise.

Indicators of success

Is supplier performance being regularly measured against defined metrics, and is this visible to board members?

Success criteria should be defined, and metrics consistently reported to the board so you have visibility of the risk levels. This may include, % of suppliers/subcontractors who have been assessed, when they were last assessed, % compliant with required policy, as well as an overview of high severity issues uncovered.

Is your organisation developing threat assessments and incident response exercises in collaboration with suppliers and partners?

If your organisation approaches cyber security in a collaborative manner, this is a good sign that you and your partners are supporting each other to enhance your cyber resilience.

Are high severity supply chain risks tracked and reported to the board?

If the board has visibility of critical issues in supply chain security, this is a good sign that it is being prioritised.

Does the organisation have a defined process for onboarding and managing suppliers?

This should include appropriate due diligence steps when initially procuring the service, along with periodic reviews and re-validation that sufficient measures are in place. For efficiency purposes, the breadth and depth of these reviews may differ and should be proportionate to the criticality of the service and the value/ sensitivity of the data involved

Are products/services provided by partners/suppliers documented?

There should be evidence that external data processing arrangements have been documented with steps in place to assure the security of data that has been shared (not just personal data). Critical dependencies on external services should be mapped ensuring the risk around external failure is within the board's appetite (or that there are credible measures in place for redress if a supplier lets your organisation down). Refer to the NCSC's guidance on How to assess and gain confidence in your supply chain cyber security.

9. Planning your response to cyber incidents

Good incident management can reduce their financial, reputational and operational impact.

Cyber security incidents (such as a data breach or ransomware infection) can have a huge impact on an organisation in terms of cost, productivity, reputation and loss of customers. Being prepared to detect and quickly respond to incidents will prevent the attacker from inflicting further damage, and can reduce the financial and operational impact.

During an incident, it's imperative the board remains operationally focussed. Handling the incident effectively whilst in the media spotlight will help to reduce the impact on your reputation and loss of customers.

Having a well-prepared cyber incident response approach is essential for cyber resilience.

The benefits include:

- key decisions and considerations can be planned in a less stressful environment and their implications properly understood
- business is restored more quickly, minimising financial losses
- legal obligations are complied with early and openly
- prompt and decisive action restores public confidence and trust, and reassures shareholders
- clear communication will alleviate fears and anxiety in the workforce
- learning from the incident and strengthening security will better prepare the organisation for future incidents

Experiencing an incident?

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

Outline case study - Ransomware attack on a large Industrial business from the eyes of its C level team.

What preparation did the organisation have in place before the attack?

The board had agreed the organisation's cyber strategy well in advance of the attack. Our cyber risks had been updated and we had carried out both technical and board-level exercises. Helpfully, we had anticipated ransomware as a potential risk and so it was one of the incidents we'd rehearsed. Underpinning this was business continuity plans across our businesses and a disaster recovery plan to support it. This level of planning undoubtedly helped us in the real event.

What were the first signs of the attack?

Our security operations team experienced an increase in alerts which were indicative of a serious threat to our systems. These were out of the ordinary and lead us to believe that an attacker had breached our network.

What was the immediate response?

The immediate response was to contain the attack on our network and systems. This alone took more than a week and was like being in a fist fight with a determined cyber criminal. Every action we took to defend our systems was met with a counter-response from the criminals.

What third party organisations did you contact for help/advice?

We engaged with external third party subject matter experts and used relationships we had built within the industry to get externally skilled resources onsite. The NCSC incident team and local law enforcement were also informed. Relationships we had built with other third parties allowed us to spend time speaking with another CEO who had experienced a devastating ransomware attack. This not only provided us with an external perspective on how impactful these types of attacks can be, but their knowledge and experience also provided myself and the board with more insights to help us lead the business out of the crisis.

Were they helpful?

Getting support from outside the organisation played a critical part in our defence and recovery. We had highly skilled internal resources but realised quickly that we would need more support to ensure we could continue defending and recovering the business without burning out our teams.

Did anything change?

We felt the tempo and intensity of the attack increase throughout the week. NCSC confirmed to us during the post-incident forensic analysis that the attack had indeed intensified and that sophisticated and determined cyber criminals were involved.

How was the morale of the team?

The general morale of the team varied as the incident progressed and this is something we had to closely monitor throughout. The team were working hard to tackle what was a particularly complex attack, in a fast-paced and fluid environment. In addition to incident containment, the team also had to address business continuity. This resulted in a stressful time for us all, and many members of the team had to spend time away from home or numerous hours on Teams calls. Where possible we tried to put measures in place to reduce the amount of business continuity tasks teams had to be involved in so they could focus on incident response. The CEO and Chair also helped to boost morale by visiting the team on a number of occasions.

When were comms issued to shareholders and customers?

Our communications strategy was multi-faceted so that we could ensure the interests of a number of different stakeholders (employees, customers, shareholders, suppliers, relevant regulators) were met.

No customer data was compromised, however, we did notify customers where appropriate where it was determined that delivery times would be impacted.

Did you pay the ransom?

No. We did not engage with the ransomware attackers at all. We disrupted the attack, and felt that we could recover without having to engage with the cyber criminals. We had confidence in our team and our business that we could recover from the attack on our own terms

What was the cost to the organisation?

The organisation was impacted through deferred revenue and loss of associated profit, under-recoveries and direct costs associated with incident response, with total financial impact in the year estimated at around £25m.

Did you suffer any reputational damage?

We did not suffer any reputational damage and were able to provide more clarity and information to our stakeholders as time went on. Further details on the status of the attack and updates on the financial impact were provided in our trading updates.

Were there any lessons learned as a result of the attack and has it resulted in positive changes to the organisation?

The positive impact was that we were able to accelerate planned changes to enhance our security, and we benefitted from tailored input from external expertise.

Is there any advice you would give to other organisations regarding planning for or dealing with a ransomware attack?

Use exercises to ensure the basics are being done really well when it comes to key cyber hygiene across areas like patching and access control across your systems. It is also helpful to understand your environment as much as possible (for example, what suppliers you have in your supply chain, how they are connected to your systems, what data they have).

Essential activities

Plan your response

Ensure your organisation has an incident response plan in place as it will minimise the impact of incidents, helping normal operations to be resumed as quickly as possible. It should be regularly reviewed and maintained to ensure that it continues to be relevant as roles and structure of the organisation changes.

The incident response plan must set out:

- how the severity of an incident is determined
- delegation of authority to make key decisions
- responsibilities for contacting key individuals in the organisation (including board members), suppliers and regulators to share information about the incident

Understand your role

The quality of decision making can be compromised in times of crisis, so it is vital that everyone has a clear understanding of their role and the organisational response in advance. Responding to an incident may require making major decisions such as whether to take systems offline (for instance your public facing website, or other operationally critical systems). It is critical that people know what authority they have, especially if an incident happened outside of normal business hours. For more details about essential roles and responsibilities during incidents, please refer to the NCSC's detailed Incident Management Guidance.

Practise your plan

Exercising your incident response procedures is as important as practicing fire drills. It is no good having a procedure if no-one remembers what it is, or you only discover that part of it doesn't work when you're in the middle of a real situation.

- Board members involvement in these activities can really help (whether participating as an observer or a 'player' in the scenario) as a rehearsal for what would happen in a real event.
- Exercises can be run in a variety of ways, from 'tabletop' to more in-depth simulations, which are an excellent way of identifying areas of continuous improvement. The NCSC has produced 'Exercise in a box,' a free service that provides you with a number of scenarios, based on common cyber threats.
- It may be beneficial to involve partners and service operators in the exercise. You should also consider what you would do in the event that a supplier is compromised.

Learn lessons

An incident can provide valuable insight into your cyber readiness. You should ensure your organisation has processes for conducting post-incident analysis. This generates insight that can help you reduce the likelihood of incidents occurring in the future and reduce their potential impact. For this to work you need to be able to be honest and objective about what has happened. Consider rewarding people for being open and contributing insights into what happened. Critically for the board, 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.

Ensure you can spot events

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 when it happens, it is still useful to collect system or network logs so that you can retrospectively review them once you know an incident has occurred.

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.

Indicators of success

Does your organisation have an incident response plan in place, and do you regularly exercise it?

Board members should expect direct sight of the plan. Exercises identify improvements and are a far better way to ensure people know what they are expected to do, rather than reading documents. The board should expect to see reporting on the exercise conducted and lessons learned. If an exercise has recently taken place against the cyber risk scenarios defined in the risk register, this suggests that the key processes will be fresh in the minds of both the board and the workforce, and you are prepared for incident response.

Does every board member understand what's required during an incident?

Do you have the understanding required to make decisions potentially out of hours, and under time pressures? Do you need training to support your specific role in an incident, such as understanding relevant regulations, or dealing with the media? Is there a communications plan in place with individuals assigned to deliver the corporate message both internally and externally? Effective communication in a crisis will not only put employees at ease but also help to protect the organisation's reputation.

If a significant cyber incident has occurred in the recent past, can the person responsible for cyber security report what improvements have been made?

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.

Are cyber incidents considered in the design of your Disaster Recovery (DR) and Business Continuity Plans (BCP)?

Plans are integral to effective response. An incident response plan covers the immediate response to a cyber attack:

- a BCP addresses how your organisation will continue to operate
- a DR plan details how your organisation will get systems up and running

A ransomware attack could compromise the availability of assets in a similar way to a fire, a flood, or theft, and recovery in all these cases will depend on some combination of contingency plans, alternative sites, and backup systems. If there is mention of contingences in the plans it is a good sign your organisation is prepared. For example, if the payroll system goes down, how do you make sure that employees can pay their bills at the end of the month?

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)
- your cyber insurance provider

Cyber security regulations and directors duties in the UK

This section summarises relevant cyber security regulations that boards need to be aware of. 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.

UK General Data Protection Regulation (UK GDPR)

UK 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 your organisation will depend upon your circumstances, as well as the data you are processing and therefore the risks posed.

GDPR focuses on explicit accountability for data protection, placing a direct responsibility on companies to prove they comply with the principles of the regulation, rather than the hands-off approach of the Data Protection Act. This means firms will need to commit to mandatory activities such as staff training, internal data audits and keeping detailed documentation if they wish to avoid falling foul of the GDPR rules. Breaches must be reported to the relevant authorities within 72 hours of the incident.

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.

Data Protection Act 2018

The Data Protection Act 2018 provides guidance and best practice for data handling.

Everyone responsible for using personal data has to follow strict rules called 'data protection principles'. They must make sure the information is:

- used fairly, lawfully and transparently
- used for specified, explicit purposes
- used in a way that is adequate, relevant and limited to only what is necessary
- accurate and, where necessary, kept up to date
- kept for no longer than is necessary
- handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction or damage

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 has developed some resources that organisations affected by the NIS regulations are likely to find useful. These are:

- a set of cyber security and resilience principles for securing essential services
- a collection of supporting guidance
- a Cyber Assessment Framework (CAF) incorporating indicators of good practice

Collectively, these resources are known as the NCSC CAF collection and can be found on the website. Please note that the use of the CAF collection extends beyond organisations designated as OES by the NIS regulations. For that reason, the terminology of the CAF collection is intended to generalise and extend the terminology used in the NIS regulations.

Update to the NIS Directive

The UK Government announced that, following a public consultation in January 2022, the Network and Information Systems (NIS) Regulations (NIS Regulations) will be updated and strengthened to protect essential and digital services against increasingly sophisticated and frequent cyber-attacks (on 30 November 2022). As part of this update, outsourced IT and managed service providers (MSPs) will be brought into scope of the NIS Regulations, alongside other essential service providers, such as energy, transport, healthcare and water companies and providers of important digital services, such as cloud computing and online search engines. For more information please refer to the DCMS's response to the consultation.

Directors Duties

Directors have defined responsibilities under Section 172 of the Companies Act and must act in the company's best interests to promote its success.

You must consider the:

- consequences of decisions, including the long term
- interests of its employees
- need to support business relationships with suppliers, customers and others
- impact of its operations on the community and environment
- company's reputation for high standards of business conduct
- need to act fairly to all members of the company

The Board Toolkit will help to embed cyber resilience into all areas of the organisation.

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.

FSC
www.fsc.org
MIX
Paper from responsible sources
FSC® C113965