Board Toolkit: Questions for the board to ask about cyber security

This document briefly summarises each module of the toolkit. It then provides a series of questions (with possible answers) that boards can use to help evaluate your organisations performance.

Visit ncsc.gov.uk/board-toolkit to view and download the complete Board Toolkit.

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

Embedding cyber security into your organisation

Cyber security is not just 'good IT'. It should 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. Done well, cyber security will enable your organisation's digital activity to flourish, adding value to your business. It's also a team sport, and as Board Member, it's vital that you empower everyone.

1. 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.

2. 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 it should be reviewed at least annually or in line with current threat level.

3. 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.

4. 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.

5. 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.

6. 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.

Developing a positive cyber security culture

Security culture refers to the values that determine how people are expected to think about and approach security in an 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.

1. 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.

2. 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.

3. 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.

4. 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.

Growing cyber security expertise

As the demand for cyber security professionals grows, senior leaders should ensure that recruitment and training meet their cyber security needs. This will include a combination of investing in your people, bringing in external expertise, and developing a pipeline of talent. The assessment of cyber skills might be an activity within the people planning part of the business, and the board should have sight of this.

1. 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.

2. 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.

3. 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.

4. 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 recent Decrypting Diversity report).

5. 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.

6. 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.

Identifying the critical assets in your organisation

Understanding how technical assets are critical to your organisation's objectives is key to effective risk management. This means having a good understanding of its technical estate, and 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 in order for the technical experts to focus on protecting the things that ensure these objectives are fulfilled.

1. 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.

2. 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.

3. 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.

4. 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 (ie 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.

Understanding the cyber security threat

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). Threats will evolve over time, so it's important to stay up-to-date and regularly perform threat assessments.

1. 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.

2. 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.

3. 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.

4. 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.

Risk management for cyber security

Every organisation has to make difficult decisions around how much time and money to spend protecting their technology and services; cyber risk management should inform and improve these decisions. 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 as a standalone topic (or considered simply in terms of 'IT risk').

1. 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.

2. 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).

3. Do we have an effective approach to managing 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.

4. 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.

Implementing effective cyber security measures

Implementing effective cyber security measures will help reduce the likelihood of a significant incident. Even basic cyber security measures can reduce your exposure to cyber attacks, and lessen the associated reputational, financial and legal impacts. With a baseline of 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.

1. 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.

2. 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.

3. 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.

4. 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,

5. 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.

Collaborating with your supply chain and partners

Many organisations rely upon suppliers to deliver products, systems, and services. Supply chains are often large and complex, and effectively securing the supply chain can be hard because vulnerabilities can be inherent, introduced or exploited at any point within it. Building a clear picture of your suppliers (and working with them to establish their sub-contractors) is essential if you are to gain assurance that threats from the supply chain are understood, and risks mitigated.

1. 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.

2. 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.

3. 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.

4. 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.

5. 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.

Planning your response to cyber incidents

Cyber security incidents 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 is paramount to prevent the attacker from inflicting further damage, reducing the financial and operational impact. Having a well-prepared cyber incident response approach is essential for cyber resilience.

1. 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.

2. 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? If not a specific board member, is there a communications plan in place, with individuals assigned to deliver the corporate message, which has been approved in advance?

3. 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.

4. 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 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?

5. 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