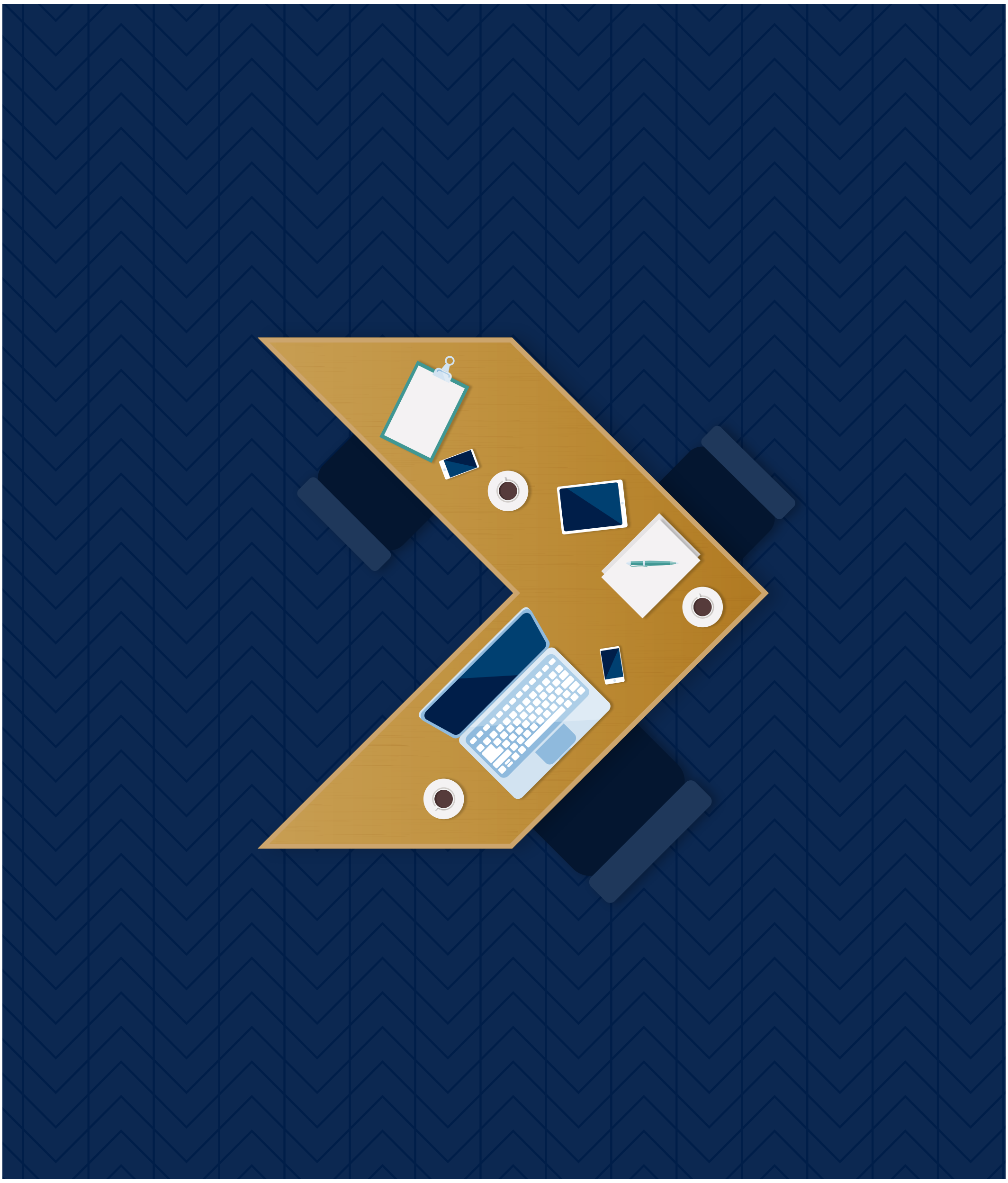
National Cyber Security Centre
a part of GCHQ

Questions for boards to ask about cyber security

Taken from the NCSC's Cyber Security Toolkit for Boards.



Contents

Introducing the Cyber Security Toolkit for Boards 3

1 - Embedding cyber security into your structure and objectives 4

2 - Growing cyber security expertise 6

3 - Developing a positive cyber security culture 8

4 - Establishing your baseline and identifying what you care about most 10

5 - Understanding the cyber security threat 12

6 - Risk management for cyber security 14

7 - Implementing effective cyber security measures 16

8 - Collaborating with suppliers and partners 18

9 - Planning your response to cyber incidents 20

About the NCSC 23

Introducing the Cyber Security Toolkit for Boards

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

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

Board members don't need to be technical experts, but they *do* need to know enough about cyber security to be able to have a fluent conversation with their experts and understand the right questions to ask. The NCSC's Board Toolkit has been created to encourage essential discussions about cyber security to take place between the board and their technical experts.

The toolkit is separated into nine modules that can be approached in any order. Each deals with an important aspect of cyber security.

What does good cyber security look like?

The NCSC is often asked 'what does good look like in terms of cyber security?' The simple answer is 'whatever protects the things you care about'.

This means that whilst there is some good practice that applies in most situations, 'good' cyber security for one organisation may not be 'good' for another.

Cyber security has to work for you: it has to be appropriate to your systems, your processes, your staff, your culture and, critically, it has to be appropriate for the level of risk you are willing to accept.

This document briefly summarises each module of the toolkit. It then provides questions that board members can use to start crucial conversations with their cyber security experts. The complete board toolkit can be viewed and/or downloaded at

https://www.ncsc.gov.uk/collection/board-toolkit/

Many questions will lead to follow on questions, and there may be a range of possible answers. You'll see that there are up to three different audiences for the questions:

- questions directed **at board members themselves**. These are for individuals to reflect on their *own* role and responsibilities.
- questions for **the board**. These might be about strategy, for example, or the collective responsibilities of the board and how these are assigned.
- questions for **the organisation as a whole**. These might be topics that the board needs to **seek assurance on** rather than needing to be familiar with the detail of the answers. A good starting point could be for the board to commission someone within the organisation to prepare a brief report on these particular questions.

The questions are only the start of the story - you may find that simply getting the right people in the room engaged in meaningful discussions can throw a light on what works (and doesn't work) within your organisation.

1 Embedding cyber security into your structure and objectives

Cyber security should be seen as an *enabler*: something that supports an organisation's overall objectives rather than a standalone issue. Cyber security impacts on every aspect of an organisation and so needs to be integrated for it to be successful. This means incorporating it in organisational risk management and decision making. Good cyber security isn't just about having good *technology*: it's also about *people* having a good relationship with security and having the right *processes* in place across the organisation to manage it.

Questions for the board

Q1

Do we understand how cyber security impacts upon our individual and collective responsibilities?

You might want to consider:

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

Q2

How do we assure ourselves that the organisation's approach to cyber security is effective?

You might want to consider whether:

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

Questions for the organisation

Q3

Who currently has responsibility for cyber security?

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

- What are their objectives and who sets them? Do these objectives drive cyber security to be an enabler for the organisation?
- Do they have access to the necessary people to ensure effective cyber security? This could simply be the resource required to meet cyber security objectives but could also be the teams they need to link in with e.g. HR, policy, finance. .
- How they engage with the board? For example, do they report directly to the board or do they fit into another reporting process? Does this arrangement encourage the board to actively participate in discussions on cyber security?

Q4

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

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

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

2 Growing cyber security expertise

Cyber skills are already in high demand, for example, the Global Information Security Workforce study[1] estimates that by 2022 there will be a shortfall of 350,000 appropriately trained and experienced individuals in Europe. Organisations must take steps now to ensure they can draw on cyber security expertise in the future. This might include a mix of developing skills in house, recruiting new staff and outsourcing specific functions.

Questions for board members

Q1

Do I have the right level of expertise to be accountable for cyber security decisions?

- Do I understand enough about the cyber security decisions being made to be accountable to shareholders?
- If not, what plan do I have in place to increase my expertise? (The Introduction to Cyber Security section of the Cyber Security Toolkit for Boards[2] is a good place to start. There are also many training providers who run sessions specifically for board level delegates.)

Questions for the organisation

Q2

What cyber expertise do we need, and what do we already have?

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

Q3

What is our plan to develop the expertise we don't currently have?

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

Q4

Are we building an equal, diverse and inclusive workforce to tackle our cyber security skills challenges?

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

[1] https://www.computerweekly.com/news/450420193/Europe-faces-shortage-of-350000-cyber-security-professionals-by-2022

[2] https://www.ncsc.gov.uk/collection/board-toolkit/introduction-cyber-security-board-members

3 Developing a positive cyber security culture

A positive security culture, where people feel safe to raise concerns and challenge ineffective practices, will help you build security that works for your organisation. Establishing and maintaining such a culture is about putting people at the heart of structures and policies. Focusing solely on the *technical* issues risks overlooking the needs of people and how they get their work done, and can result in staff finding workarounds and/or having a negative attitude towards security.

Questions for board members

Q1

Do I lead by example?

You might do this by:

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

Questions for the organisation

Q2

Do we have a good security culture?

Some signs that an organisation has a good approach could include:

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

Q3

What do we do to encourage a good security culture?

This can vary depending on the size and nature of your organisation. Examples could include:

- Properly resourced staff awareness programmes that include information on how to report security concerns or ask questions.
- Ensuring that staff input is included when creating new policies or system designs.
- Sharing *positive* security metrics rather than negative ones which might unfairly apportion blame (for example, how many people reported phishing emails rather than how many people clicked on them).
- Support from senior leadership on the importance of security.

4 Establishing your baseline and identifying what you care about most

Key to effective cyber security risk management is understanding what technical assets an organisation has and how these contribute to achieving the organisation's objectives. As with any other business risks, it's impossible to mitigate all cyber security risks all of the time, and therefore defences have to be *prioritised*. Ensuring key objectives have been communicated means that the technical experts can get on with protecting what is most essential to the organisation.

Questions for the board

Q1

Have we clearly communicated our priority objectives and do we have assurance that these priorities guide our cyber security efforts?

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

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

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

Questions for the organisation

Q2

Do we have a clear understanding of how technical systems, processes or assets are contributing to achieving our objectives?

Questions that may help in identifying these dependencies include:

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

Q3

How do we identify and keep track of the systems, data and services that we are responsible for?

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

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

5 Understanding the cyber security threat

Different organisations face different types of threat - both targeted and untargeted - from perpetrators such as cyber criminals, hostile nation states, activists and insiders. Understanding the threats faced by your own organisation - either in its own right or because of who you work with - will enable you to most effectively tailor your approach to cyber security.

Questions for the organisation

Q1

Which threats do we assess are most relevant to our organisation and why?

This assessment might:

- consider the potential motivations of those behind cyber attacks and the likelihood of them targeting your organisation
- identify and understand the risk from untargeted attacks that could affect your organisation
- inform which risks you are willing to tolerate
- be enriched by collaboration with key partners in your sector
- be supported by evidence from the attacks you have experienced to date

Q2

How do we stay up to date with the cyber threat?

You might:

- seek to discover evidence of any attacks in system logs you may hold
- subscribe to a number of threat intelligence feeds
- be part of a sector-specific intelligence sharing group, e.g. the NCSC's Cyber Security Information Sharing Partnership (**CiSP**[3])
- have mechanisms for sharing key cyber threat updates internally

Q3

How do we use threat intelligence to inform business as usual (BAU)?

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

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

[3] https://www.ncsc.gov.uk/section/keep-up-to-date/cisp

6 Risk management for cyber security

Good risk management needs to go beyond compliance: it can also provide a rich source of information about the health of your organisation. To be most effective, cyber security risk management should be integrated with your organisational approach to risk management more broadly. This ensures that the wider implications of cyber security risks are identified, as well considering how more general organisational risk may affect cyber security.

Questions for the board

Q1

Have we clearly set out what types of risks we would be willing to take and those which are unacceptable?

- Are we specific about the *types* of risk as well as the *amount* of risk we are willing to take? For example, we might be unwilling to tolerate any significant risk to personal data but willing to accept email being unavailable for a day.

- Do we consider the *cumulative* risk we are prepared to accept? It's possible that all your cyber risk could be realised at the same time. In a single incident, you might lose email for a day, the public website might be unavailable and financial data you hold might be stolen. Whilst you may have accepted some risk of all of those things happening, you may not have considered whether the organisation could tolerate them all happening at once.

- Do we support decision makers when they make risk decisions within the parameters we have previously set?

- Are we clear about when and how we expect a risk to be escalated to the board? (see also Q4)

Questions for the organisation

Q2

Do we have a process that means decision makers are as well informed as possible?

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

Q3

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

Any decision maker in the organisation should have an awareness of the importance of cyber security risk and also enough expertise - or access to expertise - to consider cyber security risk in the decisions they make.

To begin to integrate cyber risk into business risk decisions, an organisation might want to:

- consciously build in consideration of cyber security risk to any decision-making processes in use

- focus on educating people on cyber security

It is possible to review whether cyber risk is being balanced with other business risks by looking back on a decision and considering which (if any) cyber risks were considered in the process, and whether these were taken into account as *part* of decision making or only once the business decision had been made.

Q4

Do we have an effective and appropriate approach to managing cyber risk?

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

- how risks are escalated

- the threshold for board involvement in a risk decision

- how confidence in a particular risk assessment is conveyed

- how often risks are reviewed

- who owns which risks

- who is responsible for the cyber risk framework itself and for ensuring it is fit for purpose (e.g. ensuring that the output of a risk assessment process genuinely reflects the assessment of the risk rather than telling leaders what they want to hear)

7 Implementing effective cyber security measures

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

Implementing a baseline of cyber security controls from a suitable framework is often a good place to start and then defences can be tailored to mitigate against the highest priority risks. As the needs of the organisation and the profile of the threat changes, it's important to have some way to assess whether defences continue to be effective.

Questions for the organisation

Q1

How do we assure ourselves that our cyber security measures are effective?

You might seek this assurance through:

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

Q2

What measures do we take to minimise the damage an attacker could do inside our network?

You might consider:

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

Further details on these points is provided in NCSC guidance on **preventing lateral movement**[4].

Q3

Do we implement cyber security controls to defend against the most common attacks?

How do we defend ourselves against phishing attacks?

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

How do we control the use of privileged IT accounts?

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

How do we ensure that our software and devices are up to date?

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

Which authentication methods do we use to control access to systems and data?

- We take measures to encourage the use of sensible passwords (for example, encouraging people to consider using the 'three random words' technique for choosing passwords, blacklisting common passwords and avoiding setting ineffective complexity rules for password format).
- We ensure password requirements don't put a disproportionate burden on staff.
- We implement two factor authentication (2FA) where possible.

[4] https://www.ncsc.gov.uk/guidance/preventing-lateral-movement

8 Collaborating with suppliers and partners

Cyber attacks on your suppliers can be just as damaging as an attack on your own networks. Cyber security considerations should therefore be taken into account in any decisions taken about new relationships or collaborations, whether that's suppliers, providers, mergers, acquisitions or partnerships.

Questions for the board

Questions for the organisation

Q1

Do we have a clear strategy for using suppliers, and have we communicated it?

If procurement and supplier decisions are devolved below the board, has the board clearly communicated:

- What risk you are willing to accept in using suppliers? For example, if your organisation is compromised through a supply chain attack, you may not be exposed to the same level of reputational risk as if you were directly compromised, but you may be exposed to the same level of financial risk.
- What are your expectations of suppliers' security and how much you are willing to pay for better security? For example, if company A is more expensive but more secure, how much cheaper would company B need to be to make this the preferred option?
- What opportunities you are trying to exploit? This should be supported by an awareness of what you are able to cater for within your organisation and what you will outsource. For example, if you assess it's not feasible to support your own data storage, do you take advantage of the competitive cloud data storage market?
- What is your appetite for working with partners or suppliers overseas? Some jurisdictions are incompatible with UK security and regulatory requirements or may bring very different continuity of supply issues. For further considerations see CPNI's **Secure Business**[5] guidance.

[5] https://www.cpni.gov.uk/secure-business

Q2

How do we mitigate the risks associated with sharing data and systems with other organisations?

Organisations should:

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

To do this you might:

- Agree processes with your main suppliers on how they subcontract any work, specifically what obligations they have to inform you of these subcontractor arrangements and of any significant incidents in the supply chain.
- Choose organisations that can demonstrate the security of their own defences. For example, larger organisations will have carried out regular penetration tests and responded to the findings to understand their residual vulnerability. SME's might have been certified under the government's Cyber Essentials scheme.
- Limit services and information exchanged with other organisations to the minimum necessary.
- Implement user and system authentication and authorisation before access is granted.
- Audit any sensitive actions or data exchange/access.

Q3

How do we ensure that cyber security is considered in every decision made about collaboration and/or working with partners?

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

Q4

Are we confident that we are fulfilling our security requirements as a supplier?

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

As a supplier you should:

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

9 Planning your response to cyber incidents

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

Questions for board members

Q1

Do I understand my role during an incident and have I had training to equip me?

Consider:

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

Questions for the board

Q2

Do we know who leads on an incident and who has the authority to take any decisions?

This will depend on your organisational structure. Responsibility might sit with one member of the board, or one of the executives, or it might be divided out across different roles.

Ideally you should:

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

Questions for the organisation

Q3

Do we have an incident management plan, and how do we ensure it is effective for cyber incidents?

A basic plan should include:

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

Q4

How would we know when an incident occurred?

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

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

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

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

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

9 Planning your response to cyber incidents (cont.)

Questions for the organisation

Q5

Do we know where to go for help in an incident?

This might include:

- Incident response providers (you might want to consider NCSC **Certified Incident Response**[6] companies)
- NCSC **Incident Management**[7] team, or if you think you have been the victim of online fraud, Action Fraud[8].
- Intelligence sharing groups, for details of other companies experiencing the same incident: for example, you might be a member of **CiSP**[9], the NCSC's Cyber Security Information Sharing Partnership.

Q6

How do we learn from incidents and near misses?

It's important to learn lessons from incidents as well as from 'near-misses'. These will give you valuable insight into the threat you're facing, the effectiveness of your defence, and potential issues with your policies or culture. A good organisation will use this insight to respond better to future incidents, and not seek to apportion blame.

The board may decide it doesn't need to know the details of every incident, just the most significant lessons learned from the incidents experienced.

[6] https://www.ncsc.gov.uk/information/cir-cyber-incident-response

[7] https://www.ncsc.gov.uk/section/about-ncsc/incident-management

[8] https://www.actionfraud.police.uk/

[9] https://www.ncsc.gov.uk/section/keep-up-to-date/cisp

About the NCSC

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

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

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

Help with cyber incidents

- If you are reporting a **fraud or cyber crime**, please refer to the Action Fraud[10] website.
- If you have been subject to personal data breach that is required to be reported under **GDPR**, please contact the ICO[11] (Information Commissioner's Office). If there is mailicious cyber activity related to this which you wish to report (either for information or for action), please complete an the NCSC Incident Form.

Keep up to date

- The NCSC publishes its guidance on its website – www.ncsc.gov.uk

@NCSC

National Cyber Security Centre

Are both good ways to keep up to date with new publications.

[10] https://www.actionfraud.police.uk/

[11] https://ico.org.uk/

For further information, or to contact us, please visit: **www.ncsc.gov.uk**

@NCSC

National Cyber Security Centre

@cyberhq

Information correct at the time of publication - April 2020

Designed and created by Agent Marketing Ltd.
agentmarketing.co.uk