GUIDANCE

10 Steps to Cyber Security

Guidance on how organisations can protect themselves in cyberspace.

IN THIS GUIDANCE

PUBLISHED

11 May 2021

REVIEWED

11 May 2021

VERSION

1.0

WRITTEN FOR

Cyber security professionals

Risk management

Take a risk-based approach to securing your data and systems.

Taking risks is a natural part of doing business. Risk management informs decisions so that the right balance of threats and opportunities can be achieved to best deliver your business objectives. Risk management in the cyber security domain helps ensure that the technology, systems and

information in your organisation are protected in the most appropriate way, and that resources are focussed on the things that matter most to your business. A good risk management approach will be embedded throughout your organisation and complement the way you manage other business risks.

What are the benefits?

Good risk management:

- **informs and improves decision-making**
- **helps decision-making to be delegated throughout your organisation while maintaining appropriate board-level oversight**
- **provides a foundation to adapt and respond effectively to new threats and opportunities as they emerge**

Whether you are new to cyber risk management, or you are trying to assess the efficacy of your existing approach, this guidance will help you build an understanding of what a good approach to risk management looks like, in the context of **your** organisation.

What should you do?

Think about the wider context in which you want to manage cyber risk.

- Think about what your organisation does, and what it cares about. What are the business priorities and objectives? This may seem a strange starting point for cyber security but it sets the scene for your cyber risk management. Cyber risk management is not separate to what your organisation wants to achieve but should support your organisational objectives. Thinking about the risks you would (or would not) be willing to take with technology to achieve your aims and objectives will help you make decisions about the steps to take to manage the cyber security risk.
- Consider what governance structures are in place to manage other types of business risk. How does managing and communicating

about cyber risk fit within those structures? Effective governance is important for good cyber security risk management because it controls and directs the activities and actions an organisation takes to manage the cyber security risks it faces. Your approach to managing cyber security related risks should be governed effectively in ways that work for your organisation.

- Ensure that the organisation has adequate policies approved and owned by the board that set out the risk management strategy for the organisation as a whole, and that cyber security is considered in other organisational policies where appropriate. You should ensure that your board collectively has a good enough understanding of cyber security that they understand how cyber security supports their overall organisational objectives. They should get the information they need, in a format that they understand, at the time they need it to enable decision-making.

Understand where you need to apply cyber risk management

- Think about the range of technology, systems, services and information that your organisation uses and relies on to achieve its organisational goals and priorities. You should use a variety of sources of information to help you identify this scope. For example, for existing systems you could use asset registers and system diagrams; for systems in development you can start with high level designs. Talking to those who use, manage or are affected by the systems or services will also give you useful insights into what you want to protect, and why. For further information see our Asset Management step to help you get started.
- Remember to include elements that may be outside of your direct control, but are still part of your wider risk concerns (such as your supply chain, use of third party services and cloud services.
- Don't forget to think about how people interact with technology, systems and services. How they are supported to do this in secure and usable ways contributes to your management of the organisation's cyber security risks. Systems involve people, processes and technology and your

approach to cyber risk management should take account of these different elements and how they interact with each other.

Choose a cyber security risk management approach that is right for your organisation

- Think about what approach to cyber security risk management, or mix of approaches, is right for your organisation. There are numerous tools, methods, frameworks and standards to choose from - some may be stipulated for you through standards or regulations, some you need to pay for, others are free to use. It is important that you choose an approach that is right for your business and one that will reveal good risk information about your systems and services.
- Understand that it is not always necessary to carry out a detailed risk assessment. For example, you could use a baseline such as Cyber Essentials to provide information on the basic controls needed to protect your organisation against most common internet-based attacks. However, using a baseline such as Cyber Essentials on its own has its limitations in that only the risks generally considered by the Cyber Essentials scheme will be covered by its recommended controls. They have not been designed to manage all cyber security related risks that your organisation may face. To gain a more tailored perspective, organisations will need to conduct risk analysis and assessment for themselves to address their own specific needs.
- Different methods provide different perspectives on risk. You will need to use a mix of methods and approaches to provide you with the best possible view of the risks you face.

Understand the risks you face and how to manage them

- Use your chosen approach to identify, analyse, assess and prioritise risks and make decisions on how you are going to manage them. For example, are you going to mitigate a risk by applying some technical or non-technical control? Are you going to accept a risk and carry on without taking any further action to mitigate it? Are you going to transfer a risk to someone else (for example by considering cyber security insurance)? Or

are you going to avoid a risk by changing what you do to eliminate the chance the risk occurring?

- Ensure you are taking into consideration a wide variety in risk information, and seek out information from experts or trusted sources of information. You could also consider joining knowledge sharing partnerships within industry and government (such as the CiSP Information Sharing Platform, which allows UK organisations to share cyber threat information in a secure and confidential environment).
- Remember that if you have chosen to apply controls to manage risk, you should ensure that those controls are proportionate to the risk, usable and do not adversely affect the way the business works.

Communicate effectively about cyber risks and cyber risk management

- Make sure that you effectively communicate your risk management approach to staff and decision makers, so that they understand how cyber security risks should be managed and to help them make decisions about them.
- Ensure that you communicate cyber risk in a way that fits in with how your organisation talks about other types of risk (such as legal or financial risk).
- Make sure you use meaningful language and fully explain any risk labels or scores you use. Using meaningless or poorly communicated labels can lead to misinterpretation and misunderstanding. For example, is everyone's interpretation of what constitutes a Medium risk the same across your organisation?

Apply and seek confidence in the controls you have chosen

- Apply the controls you've chosen to mitigate risk to your systems and services. The following steps in this collection may help you to apply appropriate security controls and mitigations: architecture and configuration, vulnerability management, identity and access management, data security, and logging and monitoring.
- Ensure that you understand what risks remain after you have applied the controls. Whether you are applying a set of controls

that are bespoke to your organisation's risks or are based on a baseline such as Cyber Essentials, it is not possible to entirely eliminate risk. The remaining risk (known as residual risk), should be understood by those responsible and accountable for the risk within your organisation.

- Seek confidence that the package of mitigation measures you put in place have effectively managed the risk you identified, and consider how you will maintain that confidence as your systems are used into the future.

Continually improve your approach to risk management

- Remember that risk management is an iterative process. Technology changes, as does the business environment and their associated threats and opportunities.
- Regularly review your risks to ensure that the ways you have decided to manage them remain effective and appropriate. In particular, you should revisit your risk assessments when something significant changes. This may be when there is a change in the threats you face, or when you change the technology used to deliver and manage a system or service, or the way you use a system changes significantly.
- You will also need to review the methods, frameworks and tools you use for risk management to ensure they continue to be effective in your business context and in the face of a continuously evolving cyber security and threat landscape.

Learn more

Cyber security toolkit for boards
Resources designed to encourage essential cyber security discussions between the Board and their technical experts.

Risk management guidance
Guidance to help organisations make decisions about cyber security risk.

Cloud security guidance
Guidance on how to configure, deploy and use cloud services securely.

10 Steps to

Engagement

← Cyb...

and training →

Topics

Operational security Risk management

PUBLISHED

11 May 2021

REVIEWED

11 May 2021

VERSION

1.0

WRITTEN FOR ⓘ

Cyber security professionals

Also see

Weekly Threat Report 23rd July 2021

The NCSC's weekly threat report is drawn from recent open source...

Report
23 July 2021

The first Certified Cyber Professional (CCP) Specialism is now live!

'Risk Management' is the first certifiable specialism under the...

Blog Post
8 July 2021

NCSC statement on Kaseya incident

The NCSC's official statement on the Kaseya cyber incident.

News
5 July 2021