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

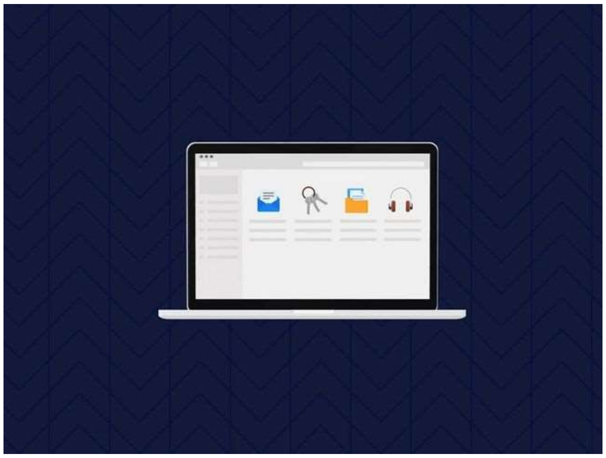
VERSION

1.0

WRITTEN FOR

Cyber security professionals

Asset management



Know what data and systems you manage, and what business need they support.

Asset management encompasses the way you can establish and *maintain* the required knowledge of your assets. Over time, systems generally grow organically, and it can be hard to maintain an understanding of all the assets within

Back to top

:. Incidents can occur as the

result of not fully understanding an environment, whether it is an unpatched service, an exposed cloud storage account or a mis-classified document. Ensuring you know about all of these assets is a fundamental precursor to being able to understand and address the resulting risks. Understanding when your systems will no longer be supported can help you to better plan for upgrades and replacements, to help avoid running vulnerable legacy systems.

What are the benefits?

- **Ability to identify what technology and information is in your organisation,**
  understand what is most important to deliver your organisation's objectives, and to assess the impact if that technology or information becomes compromised in some way.
- **Ability to identify and assess vulnerabilities that may present a risk to your organisation**
  throughout the lifetime of your systems, reducing the likelihood of a unknown system that has not been properly maintained being exploited and causing an incident
- **Ability to apply and maintain proportionate security controls**
  by having an up-to-date understanding of your assets
- **Ability to plan future technology cycles**
  to reduce the risk of legacy or unmanaged systems, as you can plan to replace these before they becomes a security risk.

What should you do?

Integrate asset management into your organisation

- Think about how asset information supports your cyber security activities such as risk management, vulnerability management and logging & monitoring. Identifying the use cases for asset information will help you understand what outcomes you require ering your approach to asset

Back to top

management. For each use case, you should consider what asset information is required, and the people and systems that are involved.

- Ensure there is responsibility for the integration and coordination of asset management across the organisation. Consider how cyber security use cases for asset management relate to other use cases such as software licensing, IT configuration management, service delivery, finance and logistics. Security is rarely considered the primary use for asset information, so a coordinated approach helps to ensure that your asset management processes meet the needs of your cyber security use cases.
- Look to design an approach that is streamlined, automated and reduces bureaucracy. If the processes and systems are hard to use or require a lot of effort by the end user, they are unlikely to get the full support of the wider organisation. This may result in workarounds that lead to duplication of effort and inaccurate records. For example, a virtual machine might not be scanned for vulnerabilities because it's too difficult for the user to register it for scanning. Or a web server may miss critical updates because the administrator mis-typed the details.

Understand your critical services and functions and identify the associated data and technology dependencies so you can prioritise these

- Create and maintain an asset inventory. Your inventory will help ensure all your assets are accounted for and should contain the information needed to support your cyber security use cases such as risk management and vulnerability management. This information does not have to be stored in one place and could be distributed based on your needs. For example, individual inventories could be managed for each system. You should use automated approaches to help ensure your asset information is accurate, kept up to date, and consistent.
- Understand what technology assets you have, including hardware, software, firmware, peripheral devices and removeable media. You should record who is responsible for

Back to top

nd what it is used for. This can

help you identify critical technology assets and where vulnerabilities may exist in your environment.

- Understand what data you have and where it is stored and processed, including more unexpected places like back-ups, local cache and downloads. You should record the person responsible for the security of data assets (usually know as a Data Owner or Information Asset Owner). Consider using a data classification scheme to help identify sensitive information and ensure appropriate protections are in place (such a scheme may be mandated in certain sectors).
- Understand what internal and external accounts you have, and the value they represent to an attacker. For example, consider the potential impact of someone else being able to impersonate your organisation on social media, or to take control of your domain name. You should understand how your organisation's identity and data is being used online, including identifying where shadow services (which are more likely to be used without sufficient oversight) are used.
- Help your staff to manage their own digital footprints, particularly senior management, board members, or staff with privileged accesses who are likely to be more attractive targets for attackers. Publicly available information about your organisation and staff can be used to make phishing messages more convincing.
- Understand the architecture of your existing systems. This may include maintaining architecture diagrams, and should include understanding where the important trust boundaries are within your systems, particularly the internet-connected or third party-facing systems and networks, and cloud services.
- Maintain a list of suppliers and what assets they hold for you. Ensure these are captured in risk assessments so that critical dependencies and significant risks can be managed. Ensure relevant contact details are held and are accessible during an incident.

Improve and validate your knowledge

Back to top

- Consider a variety of information sources for your asset management system. There are likely to be many existing sources of asset information within your environment, for example configuration management tools and mobile device management systems as well as non-technical sources such as procurement records. Each potential source may provide different properties, such as the level of detail, ease of collection or how accurate and up to date the information is, and so a combination of sources will help generate a comprehensive and accurate view.

- Use your logging and monitoring capabilities (or other asset discovery tools) to help identify unknown assets and reduce the chances of missing anything. This approach may be particularly helpful in scenarios where there are significant gaps in knowledge because the asset management capability is not very mature.

- Recognise that you are unlikely to have a complete understanding of your organisation's assets. You should be able to collect very detailed data from large homogeneous systems, such as a typical enterprise desktop environment. However, this is more challenging in diverse environments, such as research labs or OT systems. The benefits of collecting specific details should always be considered in relation to the cost of doing so. Where it is less practical to collect a full range of data, other controls such as network separation should be considered, to mitigate the resulting risks.

- Have a plan to validate your asset management system. For example, you should test your system to ensure unauthorised devices or non-compliant software configurations can be detected. This validation helps ensure that your understanding of your systems and data is accurate and therefore that you are not exposed to unidentified risks.

Only keep what you really need

- Ensure you can articulate how the above systems and data link back to your organisational purpose and strategy, and [illegible] e business owner of those

Back to top

systems is aligned with the owner of the corresponding business objectives.

- Decommission any systems or information that are no longer used or that can't be linked to a business need. Ensure that data is removed and any corresponding accounts or credentials are disabled as part of the decommissioning process. Assets that are no longer required become liabilities because they can open up vulnerabilities or expose information without any corresponding benefit, so cleaning up helps to reduce unnecessary risks.

Learn more

Asset management
Help understanding what good asset management looks like from a cyber security perspective and some of the challenges it presents.

Social media: protecting what you publish
How to reduce the likelihood of unauthorised content appearing within your organisation's social media channels.

Drawing good architecture diagrams
Some tips on good diagram drafting and pitfalls to avoid when trying to understand a system in order to secure it.

← Engagement and training

Architecture and... →

Topics

Operational security

Risk management

Asset management

PUBLISHED

11 May 2021

REVIEWED

11 May 2021

VERSION

1.0

WRITTEN FOR ⓘ

Cyber security professionals

Back to top

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

Back to top