**10 pieces of technical advice you should consider putting in place**

## **Risk Management Regime**

Why defining and communicating your Board’s Information Risk Management Regime is central to your organisation’s overall cyber security strategy.

## **Secure Configuration**

Having an approach to identify baseline technology builds and processes for ensuring configuration management can greatly improve the security of systems. You should develop a strategy to remove or disable unnecessary functionality from systems, and to quickly fix known vulnerabilities, usually via patching. Failure to do so is likely to result in increased risk of compromise of systems and information.

## **Home and mobile working**

Mobile working and remote system access offers great business benefits but exposes new risks that need to be managed. You should establish risk based policies and procedures that support mobile working or remote access to systems that are applicable to users, as well as service providers.

## **Incident management**

All organisations will experience security incidents at some point. Investment in establishing effective incident management policies and processes will help to improve resilience, support business continuity, improve customer and stakeholder confidence and potentially reduce any impact.

## **Malware prevention**

Malicious software, or malware is an umbrella term to cover any code or content that could have a malicious, undesirable impact on systems. Any exchange of information carries with it a degree of risk that malware might be exchanged, which could seriously impact your systems and services. The risk may be reduced by implementing appropriate security controls as part of an overall 'defence in depth' approach.

## **Managing user privileges**

Giving users unnecessary system privileges or data access rights means that if the account is misused or compromised the impact will be more severe than it needs to be.

## **Monitoring**

System monitoring provides a capability that aims to detect actual or attempted attacks on systems and business services. Good monitoring is essential in order to effectively respond to attacks. In addition, monitoring allows you to ensure that systems are being used appropriately in accordance with organisational policies. Monitoring is often a key capability needed to comply with legal or regulatory requirements.

## **Network security**

The connections from your networks to the Internet, and other partner networks, expose your systems and technologies to attack. By creating and implementing some simple policies and appropriate architectural and technical responses, you can reduce the chances of these attacks succeeding (or causing harm to your organisation). Your organisation's networks almost certainly span many sites, and the use of mobile / remote working, and cloud services, makes defining a fixed network boundary difficult. Rather than focusing purely on physical connections, think also about where your data is stored and processed, and where an attacker would have the opportunity to interfere with it.

## **Removable media controls**

Removable media provide a common route for the introduction of malware and the accidental or deliberate export of sensitive data. You should be clear about the business need to use removable media and apply appropriate security controls to its use.

## **User education and awareness**

Users have a critical role to play in their organisation’s security and so it's important that security rules and the technology provided enable users to do their job as well as help keep the organisation secure. This can be supported by a systematic delivery of awareness programs and training that deliver security expertise as well helping to establish a security-conscious culture.

**Risk Management Regime**

Why defining and communicating your Board’s Information Risk Management Regime is central to your organisation’s overall cyber security strategy.

**Summary**

Organisations rely on technology, systems and Information to support their business goals. It is important that organisations apply a similar level of rigour to assessing the risks to its technology, systems and information assets as it would to other risks that might have a material business impact, such as regulatory, financial or operational risks. This can be achieved by embedding an appropriate risk management regime across the organisation, which is actively supported by the board, senior managers and an empowered governance structure.

Defining and communicating the organisation’s attitude and approach to risk management is crucial. Boards may wish to consider communicating their risk management approach and policies across the organisation to ensure that employees, contractors and suppliers are aware of the organisation’s risk management boundaries.

**What is the risk?**

Taking risk is a necessary part of doing business in order to create opportunities and help deliver business objectives. For any organisation to operate successfully it needs to address risk and respond proportionately and appropriately to a level which is consistent with what risks an organisation is willing, or not, to tolerate. If an organisation does not identify and manage risk it can lead to business failure.

The lack of an effective risk management and governance structure may lead to the following:

* **Exposure to risk:** Without effective governance processes the Board will be unlikely to understand and manage the overall risk exposure of the organisation.
* **Missed business opportunities:** Risk decisions taken within a dedicated security function, rather than organisationally, will be motivated by achieving high levels of security. This may promote an overly cautious approach to risk leading to missed business opportunities or additional cost.
* **Ineffective policy implementation:** The board has overall ownership of the corporate security policy. Without effective risk management and governance processes the Board won't have confidence that its stated policies are being consistently applied across the business as a whole.

**How can the risk be managed?**

**Establish a governance framework:** A governance framework needs to be established that enables and supports a consistent and empowered approach to risk management across the organisation, with ultimate responsibility residing at board level;

**Determine what risks an organisation is willing to tolerate and what is unacceptable:** Agree what risks you are prepared to tolerate in pursuit of your business objectives. Produce guidance and statements that helps individuals throughout the organisation make appropriate risk based decisions.

**Maintain board engagement:** The board should regularly review risks that may arise from an attack on technology or systems used. To ensure senior ownership and oversight, the risks resulting from attack should be documented in the corporate risk register and regularly reviewed. Entering into knowledge sharing partnerships with other companies and law enforcement, and joining the [CiSP Information Sharing Platform](https://www.ncsc.gov.uk/cisp), can help you understand new and emerging threats as well as share approaches and mitigations that might work.

**Produce supporting policies:** An overarching technology and security risk policy should be created and owned by the board to help communicate and support risk management objectives, setting out the risk management strategy for the organisation as a whole.

**Adopt a lifecycle approach to risk management:** Technology changes, as does the threat and therefore risks change over time. A continuous through-life process needs to be adopted to ensure security controls remain effective and appropriate.

**Apply recognised standards:** Consider the application of recognised sources of security management good practice, such as the ISO/IEC 27000 series of standards.

**Make use of endorsed assurance schemes:** Consider adopting the Cyber Essentials Scheme. It provides guidance on the basic controls that should be put in place to manage risk of online cyber attack to enterprise technology and offers a certification process that demonstrates your commitment to cyber security.

**Educate users and maintain awareness:** All users have a responsibility to help manage security risks. Provide appropriate training and user education that is relevant to their role and refresh it regularly. Encourage staff to participate in knowledge sharing exchanges with peers across your organisation and beyond.

**Promote a risk management culture**: Risk management needs to be organisation-wide, driven by corporate governance from the top down, with user participation demonstrated at every level of the business.

# Secure Configuration

Having an approach to identify baseline technology builds and processes for ensuring configuration management can greatly improve the security of systems. You should develop a strategy to remove or disable unnecessary functionality from systems, and to quickly fix known vulnerabilities, usually via patching. Failure to do so is likely to result in increased risk of compromise of systems and information.

### ****Summary****

Having an approach to identify baseline technology builds and processes for ensuring configuration management can greatly improve the security of systems. You should develop a strategy to remove or disable unnecessary functionality from systems, and to quickly fix known vulnerabilities, usually via patching. Failure to do so is likely to result in increased risk of compromise of systems and information.

### ****What is the risk?****

Establishing and actively maintaining the secure configuration of systems should be seen as a key security control. Systems that are not effectively managed will be vulnerable to attacks that may have been preventable. Failure to implement good configuration and patch management can lead to the following risks:

* **Unauthorised changes to systems:**The protections you believe you have in-place may be changed by unauthorised individuals, either internal or external, leaving information at risk.
* **Exploitation of software bugs:** Attackers will attempt to exploit unpatched systems to provide them with unauthorised access to system resources and information. Many successful attacks exploit vulnerabilities for which patches have been issued but not applied.
* **Exploitation of insecure system configuration:** An attacker could exploit a system that has been poorly configured by:
  + gaining access to information they are not authorised to see
  + taking advantage of unnecessary user rights or system privilege
  + exploiting unnecessary functionality that has not been removed or disabled
  + connecting unauthorised equipment that is then able to compromise information or introduce malware
  + creating a back door to use in the future for malicious purposes

### ****How can the risk be managed?****

Organisations need to ensure that they have put in place measures to minimise the risk of poor system configuration. The following security controls should be considered:

**Use supported software:** Use versions of operating systems, web browsers and applications that are vendor (or community) supported.

**Develop and implement policies to update and patch systems:**Implement policies to ensure that security patches are applied in an appropriate time frame, such a 14 days for critical patches. Automated patch management and software update tools might be helpful. In cases where it is not possible to patch a vulnerability steps should be taken to make it very difficult to exploit. This might include making it difficult for an attacker to communicate with the system.

**Create and maintain hardware and software inventories:** Create inventories of all authorised hardware and software used across the organisation. Ideally the inventory should capture the physical location, business owner and purpose of hardware together with the version and patch status of all software. Tools can be used to help identify unauthorised hardware or software.

**Manage your operating systems and software:** Implement a secure baseline build for all systems and components, including hardware and software. Any functionality or application that does not support a user or business need should be removed or disabled. The secure build profile should be managed by a configuration control process and any deviation from the standard build should be documented and approved.

**Conduct regular vulnerability scans:**Regularly run automated vulnerability scanning tools against all networked devices and remedy or manage any identified vulnerabilities within an agreed time frame.

**Establish configuration control and management:**Implement policies that set out a configuration control and change management process for all systems.

**Disable unnecessary peripheral devices and removable media access**: Assess the need for access to peripheral devices and removable media. Disable ports and system functionality that does not support a user or business need.

**Implement white-listing and execution control**: Create and maintain a whitelist of authorised applications and software that can be executed. In addition, systems should be capable of preventing the installation and execution of unauthorised software by employing process execution controls.

**Limit user ability to change configuration:** Provide users with the permissions that they need to fulfil their business role. Users with ‘normal’ privileges should be prevented from installing or disabling any software or services running on the system.

**Limit privileged user functionality:** Ensure that users with privileged system rights (administrators) have constrained internet and email access from their privileged account. This limits exposure to spear phishing and reduces the ability of an attacker to achieve wide system access through exploiting a single vulnerability.

### Learn more

* Read our End User Device Security Guidance for recommendations on configuring modern devices.
* Our [Approaching enterprise technology](https://www.ncsc.gov.uk/guidance/approaching-enterprise-technology-cyber-security-mind) with cyber security in mind guidance contains useful guides on a range of technologies which can help to secure your organisation.
* This [Vulnerability management guidance](https://www.ncsc.gov.uk/guidance/vulnerability-management) has pointers on how to ensure problems in software and hardware products don't cause you problems.

# Home and mobile working

Mobile working and remote system access offers great business benefits but exposes new risks that need to be managed. You should establish risk based policies and procedures that support mobile working or remote access to systems that are applicable to users, as well as service providers.

## Summary

Mobile working and remote system access offers great business benefits but exposes new risks that need to be managed. You should establish risk based policies and procedures that support mobile working or remote access to systems that are applicable to users, as well as service providers.

## **What is the risk?**

Mobile working and remote access extends the transit and storage of information (or operation of systems) outside of the corporate infrastructure, typically over the Internet. Mobile devices will also typically be used in spaces that are subject to additional risks such as oversight of screens, or the theft/loss of devices. Organisations that do not establish sound mobile working and remote access practices might be vulnerable to the following risks:

* **Loss or theft of the device:** Mobile devices are highly vulnerable to being lost or stolen, potentially offering access to sensitive information or systems. They are often used in open view in locations that cannot offer the same level of physical security as your own premises.
* **Being overlooked:** Some users will have to work in public open spaces, such as on public transport, where they are vulnerable to being observed when working. This can potentially compromise sensitive information or authentication credentials.
* **Loss of credentials:** If user credentials (such as username, password, or token) are stored with a device used for remote working or remote access and it is lost or stolen, the attacker could use those credentials to compromise services or information stored on (or accessible from) that device.
* **Tampering:** An attacker may attempt to subvert the security controls on the device through the insertion of malicious software or hardware if the device is left unattended. This may allow them to monitor all user activity on the device, including authentication credentials.

## **How can the risk be managed?**

**Assess the risks and create a mobile working policy**: Assess the risks associated with all types of mobile working and remote access. The resulting mobile security policy should determine aspects such as the processes for authorising users to work off-site, device provisioning and support, the type of information or services that can be accessed or stored on devices and the minimum procedural security controls. The risks to the corporate network or systems from mobile devices should be assessed and consideration given to an increased level of monitoring on all remote connections and the systems being accessed.

**Educate users and maintain awareness:** All users should be trained on the use of their mobile device for the locations they will be working in. Users should be supported to look after their mobile device and operate securely by following clear procedures. This should include direction on:

* secure storage and management of user credentials
* incident reporting
* environmental awareness (the risks from being overlooked, etc.)

**Apply the secure baseline build:** Develop and apply a secure baseline build and configuration for all types of mobile device used by the organisation. Consider integrating the security controls provided in the [End User Device](https://www.ncsc.gov.uk/collection/end-user-device-security) guidance into the baseline build for mobile devices.

**Protect data at rest:** Minimise the amount of information stored on a mobile device to only that which is needed to fulfil the business activity that is being delivered outside the normal office environment. If the device supports it, encrypt the data at rest.

**Protect data in transit:** If the user is working remotely the connection back to the corporate network will probably use the Internet. All information exchanged should be appropriately encrypted. See [Using IPsec to Protect Data](https://www.ncsc.gov.uk/guidance/using-ipsec-protect-data) and [Using TLS to protect data](https://www.ncsc.gov.uk/guidance/tls-external-facing-services).

**Review the corporate incident management plans**: Mobile working attracts significant risks and security incidents will occur even when users follow the security procedures. The incident management plans should be sufficiently flexible to deal with the range of security incidents that could occur, including the loss or compromise of a device. Ideally, technical processes should be in place to remotely disable a device that has been lost or at least deny it access to the corporate network.

# Incident management

All organisations will experience security incidents at some point. Investment in establishing effective incident management policies and processes will help to improve resilience, support business continuity, improve customer and stakeholder confidence and potentially reduce any impact.

## **Summary**

All organisations will experience security incidents at some point. Investment in establishing effective incident management policies and processes will help to improve resilience, support business continuity, improve customer and stakeholder confidence and potentially reduce any impact.

## **What is the risk?**

Security incidents will inevitably happen and they will vary in their level of impact. All incidents need to be managed effectively, particularly those serious enough to warrant invoking the organisation’s business continuity or disaster recovery plans. Some incidents can, on further analysis, be indicative of more severe underlying problems.

If businesses fail to implement an incident management capability to detect, manage and analyse security incidents the following risks could be realised:

* **Managing business harm:**Failure to realise that an incident is happening or has occurred limits your ability to manage it effectively. This may lead to a much greater overall business impact, such as significant system outage, serious financial loss or erosion of customer confidence.
* **Continual disruption:** An organisation that fails to address the root cause of incidents (such as poor technology or weaknesses in the corporate security approach) could be exposed to repeated or continual compromise or disruption.
* **Failure to comply with legal and regulatory reporting requirements:** An incident resulting in the compromise of sensitive information covered by mandatory reporting requirements could lead to legal or regulatory penalties.

The organisation’s business profile or role will determine the type and nature of incidents that could occur and the impact they might have, so a risk-based approach should be used to shape incident management plans.

## **How can the risk be managed?**

**Establish an incident response capability:** Identify the funding and resources to develop, deliver and maintain an organisation-wide incident management capability. Resources could be in house or you might pre-establish a relationship with an specialist incident management company. This should address the full range of incidents that could occur and set out appropriate responses. The supporting policy, processes and plans should be risk based and cover any legal or regulatory reporting requirements.

**Provide specialist training:** The incident response team may need specialist knowledge and expertise across a number of technical (including forensic investigation) and non-technical areas. You should identify recognised sources (internal or external) of specialist incident management training and maintain the organisation’s skill base.

**Define the required roles and responsibilities:** Appoint and empower specific individuals (or suppliers) to handle incidents and provide them with clear terms of reference to make decisions and manage any incident that may occur. Ensure that the contact details of key personnel are readily available to use in the event of an incident.

**Establish a data recovery capability:** Data losses can occur and so a systematic approach to the backup of essential data should be implemented. Where physical backup media is used this should be held in a physically secure location, ideally offsite. The ability to recover archived data for operational use should be regularly tested.

**Test the incident management plans:** All plans supporting security incident management (including business continuity and disaster recover plans) should be regularly tested. The outcome of the tests should be used to inform the future development of the incident management plans.

**Decide what information will be shared and with whom:** For services or information bound by specific legal or regulatory reporting requirements you may have to report incidents. All internal and external reporting requirements should be clearly identified in the incident management plan.

**Collect and analyse post-incident evidence**: The preservation and analysis of the sequence of events that led up to the incident is critical to identify and remedy the root cause. The collected evidence could also potentially support any follow on disciplinary or legal action and the incident management policy should set out clear guidelines to follow.

**Conduct a lessons learned review:** Log the actions taken during an incident and review the performance of the incident management process post incident (or following a test) to see what aspects worked well and what could be improved. Review the organisational response and update any relevant policies or user training that could have prevented the incident from occurring.

**User awareness:** Users should be aware of their responsibilities and how they can report and respond to incidents. Users should be encouraged to report any security weaknesses or incident as soon as possible, without fear of recrimination.

**Report criminal incidents to law enforcement:** It is important that potential or actual cyber crime is reported to Action Fraud or other relevant law enforcement agency.

# Malware prevention

Malicious software, or malware is an umbrella term to cover any code or content that could have a malicious, undesirable impact on systems. Any exchange of information carries with it a degree of risk that malware might be exchanged, which could seriously impact your systems and services. The risk may be reduced by implementing appropriate security controls as part of an overall 'defence in depth' approach.

## **Summary**

Malicious software, or malware is an umbrella term to cover any code or content that could have a malicious, undesirable impact on systems. Any exchange of information carries with it a degree of risk that malware might be exchanged, which could seriously impact your systems and services. The risk may be reduced by implementing appropriate security controls as part of an overall 'defence in depth' approach.

## **What is the risk?**

Malware infections can cause material harm to your systems. This might include disruption of business services, unauthorised export of sensitive information or loss of access to critical data (eg caused by ransomware).The range, volume and source of information exchanged (as well as the technologies used) provide a range of opportunities for malware to be imported. Examples include:

* **Email:** Email still provides a primary path for internal and external information exchange. Malicious email attachments can cause their payload to be executed when the file is opened or otherwise processed. Email with malicious content may be specifically targeted at known individuals (known as spear phishing) with access to sensitive information, or at roles with elevated privileges. Alternatively malicious email may include embedded links that direct users to websites hosting malicious content.
* **Web browsing:**Users could browse (or be directed to) websites that may contain malicious content which seeks to compromise applications (such as the browser) that interact with that content
* **Web services:** User access to social media and other web based services could provide an ability for users to import a variety of data formats
* **Removable media and personally owned devices:** Malware can be transferred to a corporate system through the uncontrolled introduction of removable media or the direct connection of untrusted devices. This might include (for example) connecting a smartphone via a USB port, even if intended only to charge the device.

## **How can the risk be managed?**

**Develop and implement anti-malware policies:** Develop and implement corporate anti-malware policies and standards and ensure that they are consistently implemented across your infrastructure. The approach should be applicable and relevant to all business areas.

**Manage all data import and export:** All data should be scanned for malicious content at the network perimeter, whether that's internet gateways or facilities to introduce removable media.

**Deny list malicious web sites:** Ensure that the perimeter gateway uses deny listing to block access to known malicious web sites.

**Provide dedicated media scanning machines:** Stand-alone workstations can be provided and equipped with appropriate anti-virus products. The workstation should be capable of scanning the content contained on any type of media and inspect recursive content within files. Ideally every scan should be binded to a known user.

**Establish malware defences:** Malware can attack any system process or function so a technical architecture that provides multiple defensive layers (defence in depth) should be considered. This should include the following controls.

* **End user device protection:** On many platforms host based malware protection is provided by using antivirus applications. However several platforms (such as some smartphones) meet the need to protect against malware using other mechanisms such as application whitelisting. For further information see the [NCSC End User Device](https://www.ncsc.gov.uk/collection/end-user-device-security) guidance.
* Deploy antivirus and malicious code checking solutions to scan inbound and outbound objects at the network perimeter. Where host based antivirus is used it may be sensible to use different products to increase overall detection capability. Any suspicious or infected malicious objects should be quarantined for further analysis.
* Deploy a content filtering capability on all external gateways to try to prevent attackers delivering malicious code to common desktop applications such as the web browser.
* Install firewalls where appropriate, configuring them to deny traffic by default.
* If the business processes can support it, consider disabling certain browser plugins or scripting languages.
* Where possible, disable the autorun function to prevent the automatic execution of malicious code from any type of removable media. Equally, if removable media is introduced, the system should automatically scan it for malicious content.
* Ensure systems and components are [well configured](https://www.ncsc.gov.uk/collection/10-steps-to-cyber-security?curPage=/collection/10-steps-to-cyber-security/the-10-steps/secure-configuration) according to the secure baseline build and kept up to date.

**User education and awareness**: Users should understand the risks from malware and the day-to-day processes they can follow to help prevent a malware infection from occurring. The user instructions should contain the following:

* Try to stop and think before clicking on links, but don't worry if you think you've clicked on something harmful. Tell your security team as soon as possible and they will help.
* Do not connect any unapproved removable media or personally owned device to the network.
* Report any strange or unexpected system behaviour to the appropriate security team.
* Maintain awareness of how to report a security incident.

# Managing user privileges

Giving users unnecessary system privileges or data access rights means that if the account is misused or compromised the impact will be more severe than it needs to be.

## Summary

If users are provided with unnecessary system privileges or data access rights, then the impact of misuse or compromise of that users account will be more severe than it need be. All users should be provided with a reasonable (but minimal) level of system privileges and rights needed for their role. The granting of highly elevated system privileges should be carefully controlled and managed. This principle is sometimes referred to as ‘least privilege’.

## **What is the risk?**

Organisations should understand what level of access employees need to information, services and resources in order to do their job otherwise it won't be possible to manage rights appropriately. Failure to effectively manage user privileges could result in the following risks being realised:

* **Misuse of privileges:** Users could either accidentally or deliberately misuse the privileges assigned to them. This may result in unauthorised access to information to either the user or a third party or to unauthorised system changes having a direct security or operational impact.
* **Increased attacker capability:** Attackers may use redundant or compromised user accounts to carry out attacks and, if able, they may return to reuse the compromised account or possibly sell access to others. The system privileges provided to the original user of the compromised account will be available to the attacker to use which is why they particularly seek to gain access to highly privileged or administrative accounts.
* **Negating established security controls:** Where attackers have privileged system access they may make changes to security controls to enable further or future attack or might attempt to cover their tracks by making changing or audit logs.

## How can the risk be managed?

Organisations should determine what rights and privileges users need to effectively perform their duties and implement a policy of 'least privilege'.

**Establish effective account management processes:**Manage user accounts from creation, through-life and eventually revocation when a member of staff leaves or changes role. Redundant accounts, perhaps provided for temporary staff or for testing, should be removed or suspended when no longer required.

**Establish policies and standards for user authentication and access control:** A corporate password policy should be developed that seeks an effective balance between security and usability as set out in our [password guidance](https://www.ncsc.gov.uk/collection/passwords). For some accounts an additional authentication factor (such as a token) may be appropriate.

**Limit user privileges:** Users should be provided with the reasonable minimum rights and permissions to systems, services and information that they need to fulfil their business role.

**Limit the number and use of privileged accounts:** Strictly control the granting of highly privileged system rights, reviewing the ongoing need regularly. Highly privileged administrative accounts should not be used for high risk or day to day user activities, for example web browsing and email. Administrators should use normal accounts for standard business use.

**Monitor:**Monitor user activity, particularly access to sensitive information and the use of privileged account actions. Respond where activities are outside of normal, expected bounds (such as access to large amounts of sensitive information outside of standard working hours).

**Limit access to the audit system and the system activity logs:**Activity logs from network devices should be sent to a dedicated accounting and audit system that is separated from the core network. Access to the audit system and the logs should be strictly controlled to preserve the integrity of the content and all privileged user access recorded.

**Educate users and maintain their awareness:** All users should be aware of the policy regarding acceptable account usage and their personal responsibility to adhere to corporate security policies.

# Monitoring

System monitoring provides a capability that aims to detect actual or attempted attacks on systems and business services. Good monitoring is essential in order to effectively respond to attacks. In addition, monitoring allows you to ensure that systems are being used appropriately in accordance with organisational policies. Monitoring is often a key capability needed to comply with legal or regulatory requirements.

## Summary

System monitoring provides a capability that aims to detect actual or attempted attacks on systems and business services. Good monitoring is essential in order to effectively respond to attacks. In addition, monitoring allows you to ensure that systems are being used appropriately in accordance with organisational policies. Monitoring is often a key capability needed to comply with legal or regulatory requirements.

## **What is the risk?**

Monitoring provides the means to assess how systems are being used and whether they are being attacked. Without the ability to monitor your systems you may not be able to:

* **Detect attacks:** Either originating from outside the organisation or attacks as a result of deliberate or accidental user activity. Attacks may be directly targeted against technical infrastructure or against the services being run. Attacks can also seek to take advantage of legitimate business services, for example by using stolen credentials to defraud payment services.
* **React to attacks:** An effective response to an attack depends upon first being aware than an attack has happened or is taking place. A swift response is essential to stop the attack, and to respond and minimise the impact or damage caused.
* **Account for activity:** You should have a complete understanding of how systems, services and information are being used by users. Failure to monitor systems and their use could lead to attacks going unnoticed and/or non-compliance with legal or regulatory requirements.

## **How can the risk be managed?**

**Establish a monitoring strategy and supporting policies:** Develop and implement a monitoring strategy based on business need and an assessment of risk. The strategy should include both technical and transactional monitoring as appropriate. The incident management plan as well as knowledge of previous security incidents should inform the approach.

**Monitor all systems**: Ensure that all networks, systems and services are included in the monitoring strategy. This may include the use of the use of network, host based and wireless Intrusion Detection Systems (IDS). These solutions should provide both signature-based capabilities to detect known attacks, and heuristic capabilities to detect unusual system behaviour.

**Monitor network traffic**: Inbound and outbound traffic traversing network boundaries should be monitored to identify unusual activity or trends that could indicate attacks. Unusual network traffic (such as connections from unexpected IP ranges overseas) or large data transfers should automatically generate security alerts with prompt investigation.

**Monitor user activity:** The monitoring capability should have the ability to identify the unauthorised or accidental misuse of systems or data. Critically, it should be able to tie specific users to suspicious activity. Take care to ensure that all user monitoring complies with all legal or regulatory constraints.

**Fine-tune monitoring systems**: Ensure that monitoring systems are tuned appropriately to only collect events and generate alerts that are relevant to your needs. Inappropriate collection of monitoring information and generation of alerts can mask the detection of real attacks as well as be costly in terms of data storage and investigatory resources required.

**Establish a centralised collection and analysis capability:** Develop and deploy a centralised capability that can collect and analyse information and alerts from across the organisation. Much of this should be automated due to the volume of data involved, enabling analysts to concentrate on anomalies or high priority alerts. Ensure that the solution architecture does not itself provide an opportunity for attackers to bypass normal network security and access controls.

**Provide resilient and synchronised timing:** Ensure that the monitoring and analysis of audit logs is supported by a centralised and synchronised timing source that is used across the entire organisation to support incident response and investigation.

**Align the incident management policies:** Ensure that policies and processes are in place to appropriately manage and respond to incidents detected by monitoring solutions.

**Conduct a 'lessons learned' review:** Ensure that processes are in place to test monitoring capabilities, learn from security incidents and improve the efficiency of the monitoring capability.

# Network security

The connections from your networks to the Internet, and other partner networks, expose your systems and technologies to attack. By creating and implementing some simple policies and appropriate architectural and technical responses, you can reduce the chances of these attacks succeeding (or causing harm to your organisation). Your organisation's networks almost certainly span many sites, and the use of mobile / remote working, and cloud services, makes defining a fixed network boundary difficult. Rather than focusing purely on physical connections, think also about where your data is stored and processed, and where an attacker would have the opportunity to interfere with it.

## **Summary**

The connections from your networks to the Internet, and other partner networks, expose your systems and technologies to attack. By creating and implementing some simple policies and appropriate architectural and technical responses, you can reduce the chances of these attacks succeeding (or causing harm to your organisation).

Your organisation's networks almost certainly span many sites, and the use of mobile / remote working, and cloud services, makes defining a fixed network boundary difficult. Rather than focusing purely on physical connections, think also about where your data is stored and processed, and where an attacker would have the opportunity to interfere with it.

## **What is the risk?**

Networks need to be protected against both internal and external threats. Organisations that fail to protect their networks appropriately could be subject to a number of risks, including:

* **Exploitation of systems:** Ineffective network design may allow an attacker to compromise systems that perform critical functions, affecting the organisations ability to deliver essential services or resulting in severe loss of customer or user confidence.
* **Compromise of information**: A poor network architecture may allow an attacker to compromise sensitive information in a number of ways. They may be able to access systems hosting sensitive information directly or perhaps allow an attacker to intercept poorly protected information whilst in transit (such as between your end user devices and a cloud service).
* **Import and export of malware:** Failure to put in place appropriate security controls could lead to the import of malware and the potential to compromise business systems. Conversely users could deliberately or accidentally release malware or other malicious content externally with associated reputational damage.
* **Denial of service:** Internet-facing networks may be vulnerable to Denial Of Service (DOS) attacks, where access to services and resources are denied to legitimate users or customers.
* **Damage or defacement of corporate resources:** Attackers that have successfully compromised the network may be able to further damage internal and externally facing systems and information (such as defacing your organisation's websites, or posting onto your social media accounts), harming the organisation’s reputation and customer confidence.

## **How can the risk be managed?**

Produce, implement and maintain network security designs and policies that align with the organisation’s broader risk management approach. It may be helpful to follow recognised network design principles (eg ISO 27033) to help define an appropriate network architecture including both the network perimeter, any internal networks, and links with other organisations such as service providers or partners.

**Manage the network perimeter**: Manage access to ports, protocols and applications by filtering and inspecting all traffic at the network perimeter to ensure that only traffic which is required to support the business is being exchanged. Control and manage all inbound and outbound network connections and deploy technical controls to scan for malicious content:

* **Use firewalls:** Use firewalls to create a buffer zone between the Internet (and other untrusted networks) and the networks used by the business. The firewall rule set should deny traffic by default and a whitelist should be applied that only allows authorised protocols, ports and applications to exchange data across the boundary. This will reduce the exposure of systems to network based attacks. Ensure you have effective processes for managing changes to avoid workarounds.
* **Prevent malicious content**: Deploy malware checking solutions and reputation-based scanning services to examine both inbound and outbound data at the perimeter in addition to protection deployed internally. The antivirus and malware solutions used at the perimeter should ideally be different to those used to protect internal networks and systems in order to provide some additional defence in depth.

**Protect the internal network:** Ensure that there is no direct routing between internal and external networks (especially the Internet), which limits the exposure of internal systems to network attack from the Internet. Monitor network traffic to detect and react to attempted or actual network intrusions.

* **Segregate networks as sets**: Identify, group and isolate critical business systems and apply appropriate network security controls to them.
* **Secure wireless access:** All wireless access points should be appropriately secured, only allowing known devices to connect to corporate Wi-Fi services. Security scanning tools may be useful to detect and locate unauthorised or spoof wireless access points.
* **Enable secure administration:** Administrator access to any network component should properly authenticated and authorised. Make sure default administrative passwords for network equipment are changed.
* **Configure the exception handling processes:** Ensure that error messages returned to internal or external systems or users do not include sensitive information that may be useful to attackers.
* **Monitor the network:** Network intrusion detection and prevention tools should be deployed on the network and configured by qualified staff. The capabilities should monitor all traffic for unusual incoming and outgoing activity that could be indicative of an attack. Alerts generated by the system should be promptly managed by appropriately trained staff.
* **Assurance processes**: Conduct regular penetration tests of the network architecture and undertake simulated cyber attack exercises to ensure that security controls have been well implemented and are effective.

# Removable media controls

Removable media provide a common route for the introduction of malware and the accidental or deliberate export of sensitive data. You should be clear about the business need to use removable media and apply appropriate security controls to its use.

## Summary

Removable media provide a common route for the introduction of malware and the accidental or deliberate export of sensitive data. You should be clear about the business need to use removable media and apply appropriate security controls to its use.

## What is the risk?

Removable media introduces the capability to transfer and store huge volumes of sensitive information as well as the ability to import malicious content. The failure to manage the import and export of information using removable media could expose you to the following risks:

* **Loss of information:** Removable media is very easily lost, which could result in the compromise of large volumes of sensitive information stored on it. Some media types will retain information even after user deletion, placing information at risk where the media is used between systems (or when the media is disposed of)
* **Introduction of malware:** The uncontrolled use of removable media can increase the risk of introducing malware to systems.
* **Reputational damage:** The loss of media can result in significant reputational damage, even if there is no evidence of any specific data loss.

## How can the risk be managed?

**Produce corporate policies:** Develop and implement policies and solutions to control the use of removable media. Do not use removable media as a default mechanism to store or transfer information. Under normal circumstances information should be stored on corporate systems and exchanged using appropriately protected mechanisms.

**Limit the use of removable media:** Where the use of removable media is required to support the business need, it should be limited to the minimum media types and users needed. The secure baseline build should deny access to media ports by default, only allowing access to approved users.

**Scan all media for malware:**Removable media should be automatically scanned for malware when it is introduced to any system. The removable media policy could also require that any media brought into the organisation is scanned for malicious content by a standalone machine before any data transfer takes place.

**Formally issue media to users:** All removable media should be formally issued to individual users who will be accountable for its use and safe keeping. Users should not use unofficial media, such as USB sticks given away at conferences.

**Encrypt information held on media:** Sensitive information should be encrypted at rest on media. If encryption is not employed then appropriate physical protection of the media is critical.

**Actively manage the reuse and disposal of removable media:** Where removable media is to be reused or destroyed then appropriate steps should be taken to ensure that previously stored information will not be accessible. The processes will be dependent on the value of the information and the risks posed to it and could range from an overwriting process to the physical destruction of the media by an approved third party. For more information refer to [Secure sanitisation of storage media](https://www.ncsc.gov.uk/guidance/secure-sanitisation-storage-media).

**Educate users and maintain awareness:** Ensure that all users are aware of their personal responsibilities for following the removable media security policy.

# User education and awareness

Users have a critical role to play in their organisation’s security and so it's important that security rules and the technology provided enable users to do their job as well as help keep the organisation secure. This can be supported by a systematic delivery of awareness programs and training that deliver security expertise as well helping to establish a security-conscious culture.

## **Summary**

Users have a critical role to play in their organisation’s security and so it's important that security rules and the technology provided enable users to do their job as well as help keep the organisation secure. This can be supported by a systematic delivery of awareness programmes and training that deliver security expertise as well helping to establish a security-conscious culture.

## **What is the risk?**

Users have a critical role to play in helping to keep the organisation secure, but they must also be able to effectively do their jobs. Organisations that do not effectively support employees with the right tools and awareness may be vulnerable to the following risks:

* **Removable media and personally owned devices:**Without clearly defined and usable policies on the use of removable media and personally owned devices, staff may connect devices to the corporate infrastructure that might lead to the inadvertent import of malware or compromise of sensitive information
* **Legal and regulatory sanction:** If users are not aware and supported in how they handle particular classes of sensitive information, the organisation may be subject to legal and regulatory sanction
* **Incident reporting culture:** Without an effective reporting culture there will be poor dialogue between users and the security team. This is essential to uncovering near misses and areas where technology and processes can be improved, as well as reporting actual incidents.
* **Security Operating Procedures:** If security operating procedures are not balanced to support how users perform their duties, security can be seen as a blocker and possibly ignored entirely. Alternatively, if users follow the procedures carefully this might damage legitimate business activity.
* **External attack:** Since users have legitimate system accesses and rights, they can be a primary focus for external attackers. Attacks such as phishing or social engineering attempts rely on taking advantage of legitimate user capabilities and functions.
* **Insider threat:** Changes over time in an employee’s personal situation could make them vulnerable to coercion, and they may release personal or sensitive commercial information to others. Dissatisfied employees may try to abuse their system level privileges or coerce other employees to gain access to information or systems to which they are not authorised. Equally, they may attempt to steal or physically deface computer resources.

## **How can the risk be managed?**

**Produce a user security policy:** Develop a user security policy, as part of the overarching corporate security policy. Security procedures for all systems should be produced with consideration to different business roles and processes. A 'one size fits all' approach is typically not appropriate for many organisations. Policies and procedures should be described in simple business-relevant terms with limited jargon.

**Establish a staff induction process:** New users (including contractors and third party users) should be made aware of their personal responsibility to comply with the corporate security policies as part of the induction process. The terms and conditions for their employment, or contract, should be formally acknowledged and retained to support any subsequent disciplinary action.

**Maintain user awareness of the security risks faced by the organisation:** All users should receive regular refresher training on the security risks to the organisation. Consider providing a platform for users to enquire about security risks and discuss the advice they are given. On the whole, users want to do the right thing, so giving them guidance to put security advice into practice will help.

**Support the formal assessment of security skills:** Staff in security roles should be encouraged to develop and formally validate their security skills through enrolment on a recognised certification scheme. Some security related roles such as system administrators, incident management team members and forensic investigators may require specialist training.

**Monitor the effectiveness of security training:** Establish mechanisms to test the effectiveness and value of the security training provided to all users. This will allow training improvements and the opportunity to clarify any possible misunderstandings. Ideally the training provided will allow for a two-way dialogue between the security team and users.

**Promote an incident reporting culture:** The organisation should enable a security culture that empowers staff to voice their concerns about poor security practices and security incidents to senior managers, without fear of recrimination. This should be reciprocated with a culture where security professionals acknowledge that security-related effort by non-security staff is time away from their work, and is helping to protect the organisation.

**Establish a formal disciplinary process:** All staff should be made aware that any abuse of the organisation’s security policies will result in disciplinary action being taken against them. All sanctions detailed in policy should be enforceable at a practical level.