10 Steps to Cyber Security

CESG
The Information Security Arm of GCHQ

The actions and measures detailed in each of the advice sheets collectively represents a good foundation for effective information risk management. The degree of implementation of these steps will vary between organisations depending upon the risks to their individual business, however, GCHQ's recommendation is that Boards should require their CIO and CISO to be able to articulate why a particular measure is not applicable.

Home & Mobile Working
Develop a mobile working policy & train staff to adhere to it. Apply the secure baseline build to all devices. Protect data both in transit & at rest.

User Education & Awareness
Produce user security policies covering acceptable & secure use of the organisation's systems. Establish a staff training programme. Maintain user awareness of the cyber risks.

Incident Management
Establish an incident response & disaster recovery capability. Produce & test incident management plans. Provide specialist training to the incident management team. Report criminal incidents to law enforcement.

Information Risk Management Regime
Establish an effective governance structure and determine your risk appetite - just like you would for any other risk. Maintain the Board's engagement with the cyber risk. Produce supporting information risk management policies.

Managing User Privileges
Establish account management processes & limit the number of privileged accounts. Limit user privileges & monitor user activity. Control access to activity & audit logs.

Removable Media Controls
Produce a policy to control all access to removable media. Limit media types & use. Scan all media for malware before importing on to corporate system.

Monitoring
Establish a monitoring strategy & produce supporting policies. Continuously monitor all ICT systems & networks. Analyse logs for unusual activity that could indicate an attack.

Secure Configuration
Apply security patches & ensure that the secure configuration of all ICT systems is maintained. Create a system inventory & define a baseline build for all ICT devices.

Malware Protection
Produce relevant policy & establish anti-malware defences that are applicable & relevant to all business areas. Scan for malware across the organisation.

Network Security
Protect your networks against external and internal attack. Manage the network perimeter. Filter out unauthorised access & malicious content. Monitor & test security controls.

Each of the 10 areas has a two page A4 sheet with more detail

The 10 areas also tie in with the Top 20 Critical Controls for Effective Cyber Defence, as endorsed by CPNI.

BIS Department for Business Innovation & Skills

CPNI Centre for the Protection of National Infrastructure

CabinetOffice Office of Cyber Security & Information Assurance

Reducing the cyber risk in 10 critical areas

Information Risk Management Regime

- **Establish a governance framework:** Enable and support risk management across the organisation.
- **Determine your risk appetite:** Decide on the level of risk the organisation is prepared to tolerate and communicate it.
- **Maintain the Board's engagement with cyber risk:** Make cyber risk a regular agenda item. Record cyber risks in the corporate risk register to ensure senior ownership.
- **Produce supporting risk management policies:** An overarching corporate security policy should be produced together with an information risk management policy.
- **Adopt a lifecycle approach:** Risk management is a whole life process and the organisation's policies and processes should support and enable this.

Secure Configuration

- **Develop corporate polices to update and patch systems:** Establish and maintain policies that set out the priority and timescales for applying updates and patches. Create and maintain hardware and software inventories: Use automated tools to create and maintain inventories of every device and application used by the organisation.
- **Lockdown operating systems and software:** Create a baseline security build for workstations, servers, firewalls and routers.
- **Conduct regular vulnerability scans:** Run automated vulnerability scanning tools against all networked devices at least weekly and remedy any vulnerability within an agreed time frame.

Network Security

- **Police the network perimeter:** Establish multi-layered boundary defences with firewalls and proxies deployed between the untrusted external network and the trusted internal network.
- **Protect the internal network:** Prevent any direct connections to external services and protect internal IP addresses.
- **Monitor:** Use intrusion monitoring tools and regularly audit activity logs.
- **Test the security controls:** Conduct regular penetration tests and undertake simulated cyber attack exercises.

Managing User Privileges

- **Establish effective account management processes:** Manage and review user accounts from creation and modification to eventual deletion.
- **Limit the number and use of privileged accounts:** Minimise privileges for all users. Provide administrators with normal accounts for business use. Review the requirement for a privileged account more frequently than standard accounts.
- **Monitor all users:** Monitor user activity, particularly access to sensitive information and the use of privileged accounts.

User Education and Awareness

- **Produce a user security policy:** Produce policies covering the acceptable and secure use of the organisation's systems.
- **Establish a staff induction process:** New users should receive training on their personal security responsibilities.
- **Maintain user awareness of the threats:** All users should receive regular refresher training on the cyber risks to the organisation.
- **Support the formal assessment of IA skills:** Encourage relevant staff to develop and formally validate their IA Skills.

Incident Management

- **Obtain senior management approval and backing:** The Board should lead on the delivery of the incident management plans.
- **Establish an incident response and disaster recovery capability:** Develop and maintain incident management plans with clear roles and responsibilities, regularly test your plans.
- **Provide specialist training:** The incident response team should receive specialist training to ensure they have the skills and expertise to address the range of incidents that may occur.

Malware Prevention

- **Develop and publish corporate policies:** Produce policies to manage the risks to the business processes from malware.
- **Establish anti malware defences across the organisation:** Agree a corporate approach to managing the risks from malware for each business area.
- **Scan for malware across the organisation:** Protect all host and client machines with anti virus solutions that will automatically scan for malware.

Monitoring

- **Establish a monitoring strategy and supporting policies:** Implement an organisational monitoring strategy and policy based on an assessment of the risks.
- **Monitor all ICT systems:** Ensure that the solution monitors all networks and host systems (e.g. clients and servers).
- **Monitor network traffic:** Network traffic should be continuously monitored to identify unusual activity or trends that could indicate an attack.

Removable Media Controls

- **Produce a corporate policy:** Implement policy to control the use of removable media for the import and export of information.
- **Limit the use of removable media:** Limit the media types that can be used together with user and system access and the information types that can be stored on removable media.
- **Scan all removable media for malware:** All clients and hosts should automatically scan removable media. Any media brought into the organisation should be scanned for malware by a stand alone scanner before any data transfer takes place.

Home and Mobile Working

- **Assess the risks and create a mobile working policy:** The policy should cover aspects such as information types, user credentials, devices, encryption and incident reporting.
- **Educate users and maintain their awareness:** Educate users about the risks and train them to use their mobile device securely by following the security procedures.
- **Apply the secure baseline build:** All mobile devices should be configured to an agreed secure baseline build. Data should be protected in transit and at rest.

CESG
The Information Security Arm of GCHQ

Information Risk Management Regime

Summary

It is best practice for an organisation to apply the same degree of rigour to assessing the risks to its information assets as it would to legal, regulatory, financial or operational risk. This can be achieved by embedding an information risk management regime across the organisation, which is actively supported by the Board, senior managers and an empowered Information Assurance (IA) governance structure. Defining and communicating the organisation's attitude and approach to risk management is crucial. Boards may wish to consider communicating their risk appetite statement and information risk management policy across the organisation to ensure that employees, contractors and suppliers are aware of the organisation's risk management boundaries.

What is the risk?

Risk is an inherent part of doing business. For any organisation to operate successfully it needs to address risk and respond proportionately and appropriately to a level consistent with the organisation's risk appetite. If an organisation does not identify and manage risk it can lead to business failure.

A lack of effective information risk management and governance may lead to the following:

- **Increased exposure to risk:** Information risk must be owned at Board level. Without effective risk governance processes it is impossible for the Board to understand the risk exposure of the organisation. The Board must be confident that information risks are being managed within tolerance throughout the lifecycle of deployed systems or services;

- **Missed business opportunities:** Where risk decisions are being taken at junior level without effective governance and ownership back to senior levels, it may promote an overly cautious approach to information risk which may lead to missed business opportunities. Alternatively, an overly open approach may expose the organisation to unacceptable risks;

- **Ineffective policy implementation:** An organisation's Board has overall ownership of the corporate security policy. Without effective risk management and governance processes the Board will not have confidence that its stated policy is being implemented;

- **Poor reuse of security investment:** A lack of effective governance means that information risk management activities may be undertaken locally when they could be more effectively deployed at an organisational level.

BIS Department for Business Innovation & Skills
CPNI Centre for the Protection of National Infrastructure
CabinetOffice Office of Cyber Security & Information Assurance

How can the risk be managed?

Establish a governance framework: A governance framework needs to be established that enables and supports information risk management across the organisation, with ultimate responsibility for risk ownership residing at Board level;

Determine the organisation's risk appetite: Agree the level of information risk the organisation is prepared to tolerate in pursuit of its business objectives and produce a risk appetite statement to help guide information risk management decisions throughout the business;

Maintain the Board's engagement with information risk: The risks to the organisation's information assets from a cyber attack should be a regular agenda item for Board discussion. To ensure senior ownership and oversight, the risk of cyber attack should be documented in the corporate risk register; entering into knowledge sharing partnerships with other companies and law enforcement can help you in understanding new and emerging threats that might be a risk to your own business and also to share mitigations that might work;

Produce supporting policies: An overarching corporate information risk policy needs to be created and owned by the Board to help communicate and support risk management objectives, setting out the information risk management strategy for the organisation as a whole;

Adopt a lifecycle approach to information risk management: The components of a risk can change over time so a continuous through-life process needs to be adopted to ensure security controls remain appropriate to the risk;

Apply recognised standards: Consider the application of recognised sources of security management good practice, such as the ISO/IEC 27000 series of standards, and implement physical, personnel, procedural and technical measures;

Educate users and maintain their awareness: All users have a responsibility to manage the risks to the organisation's Information and Communications Technologies (ICT) and information assets. 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 business and Government;

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.

CESG
The Information Security Arm of GCHQ

Secure Configuration

Summary

By putting in place corporate policies and processes to develop secure baseline builds and manage the configuration and the ongoing functionality of all Information and Communications Technologies (ICT), organisations can greatly improve the security of their ICT systems. Good corporate practice is to develop a strategy to remove or disable unnecessary functionality from ICT systems and keep them patched against known vulnerabilities. Failure to do so is likely to result in increased exposure of the business and its ICT to threats and vulnerabilities and therefore increased risk to the confidentiality, integrity and availability of systems and information.

What is the risk?

Establishing and then actively maintaining the secure configuration of ICT systems should be seen as a key security control. ICT systems that are not locked down, hardened or patched will be particularly vulnerable to an easily preventable attack.

Organisations that fail to produce and implement corporate security policies that manage the secure configuration and patching of their ICT systems are subject to the following risks:

- **Unauthorised changes to systems:** An attacker could make unauthorised changes to ICT systems or information, compromising confidentiality, availability and integrity;

- **Exploitation of unpatched vulnerabilities:** New patches are released almost daily and the timely application of security patches is critical to preserving the confidentiality, integrity and availability of ICT systems. Attackers (using malware) will attempt to exploit unpatched systems to provide them with unauthorised access to system resources and information. Many successful attacks are enabled by exploiting a vulnerability for which a patch had been issued some months before the attack took place;

- **Exploitation of insecure system configuations:** An attacker could exploit a system configuration that has not been locked down or hardened to compromise systems and information by:

    - The import or export of information to gain unauthorised access to information assets or to import malware;
    - Exploiting unnecessary functionality that has not been removed or disabled to conduct attacks and gain unauthorised access to systems, services, resources and information;
    - Connecting unauthorised equipment to exfiltrate information or introduce malware;
    - Create a back door to use in the future for malicious purposes.

- **Increases in the number of security incidents:** Without an awareness of vulnerabilities that have been identified and the availability (or not) of patches and fixes, the business will be increasingly disrupted by security incidents.

BIS Department for Business Innovation & Skills
CPNI Centre for the Protection of National Infrastructure
CabinetOffice Office of Cyber Security & Information Assurance

How can the risk be managed?

Organisations need to ensure that they have put in place measures to minimise the risks posed by poor configuration control and insecure system configurations. The following security controls should be considered:

Develop corporate policies to update and patch systems: Use the latest versions of operating systems, web browsers and applications. Develop and implement corporate policies to ensure that security patches are applied in a timeframe that is commensurate with the organisation's overall risk management approach. Organisations should use automated patch management and software update tools;

Create and maintain hardware and software inventories: Create inventories of the authorised hardware and software that constitute ICT systems across the organisation. Ideally, suitably configured automated tools should be used to capture the physical location, the business owner and the purpose of the hardware together with the version and patching status of all software used on the system. The tools should also be used to identify any unauthorised hardware or software, which should be removed;

Lock down operating systems and software: Consider the balance between system usability and security and then document and implement a secure baseline build for all ICT systems, covering clients, mobile devices, servers, operating systems, applications and network devices such as firewalls and routers. Essentially, any services, functionality or applications that are not required to support the business should be removed or disabled. The secure build profile should be managed by the configuration control and management process and any deviation from the standard build should be documented and formally approved;

Conduct regular vulnerability scans: Organisations should run automated vulnerability scanning tools against all networked devices regularly and remedy any identified vulnerabilities within an agreed time frame. Organisations should also maintain their situational awareness of the threats and vulnerabilities they face;

Establish configuration control and management: Produce policies and procedures that define and support the configuration control and change management requirements for all ICT systems, including software;

Disable unnecessary input/output devices and removable media access: Assess business requirements for user access to input/output devices and removable media (this could include MP3 players and Smart phones). Disable ports and system functionality that is not needed by the business (which may include USB ports, Floppy/CD/DVD/Card media drives);

Implement white-listing and execution control: Create and maintain a white list of authorised applications and software that can be executed on ICT systems. In addition, ICT systems need to be capable of preventing the installation and execution of unauthorised software and applications by employing process execution controls, software application arbiters and only accepting code that is signed by trusted suppliers;

Limit user ability to change configuration: Provide users with the minimum system rights and 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.

CESG
The Information Security Arm of GCHQ

Network Security

Summary

Connecting to untrusted networks (such as the Internet) exposes corporate networks to attacks that seek to compromise the confidentiality, integrity and availability of Information and Communications Technologies (ICT) and the information they store and process. This can be prevented by developing policies and risk management approaches to protect corporate networks by applying security controls that are commensurate with the risks that have been identified and the organisation's risk appetite.

What is the risk?

Corporate networks need to be protected against both internal and external threats. The level to which networks are protected should be considered in the context of the organisation's risk appetite, risk assessment and corporate security policies.

Businesses that fail to protect their networks appropriately could be subject to a number of risks, including:

- **Leakage of sensitive corporate information:** Poor network design could be exploited by both internal and external attackers to compromise information or conduct unauthorised releases of sensitive information resulting in compromises in confidentiality, integrity and availability;
- **Import and export of malware:** Failure to put in place appropriate boundary security controls could lead to the import of malware and the compromise of business systems. In addition, users could deliberately or accidentally release malware or other malicious content to business partners or the general public via network connections that are poorly designed and managed;
- **Denial of service:** Networks that are connected to untrusted networks (such as the Internet) are vulnerable to denial of services attacks, where access to services and information is denied to legitimate users, compromising the availability of the system or service;
- **Exploitation of vulnerable systems:** Attackers will exploit poorly protected networks to gain unauthorised access to compromise the confidentiality, integrity and availability of systems, services and information;
- **Damage or defacement of corporate resources:** Attackers that have successfully compromised the network can damage internal and externally facing systems and information (such as defacing corporate websites), harming the organisation's reputation and customer confidence.

BIS Department for Business Innovation & Skills
CPNI Centre for the Protection of National Infrastructure
CabinetOffice Office of Cyber Security & Information Assurance

How can the risk be managed?

Produce, implement and maintain network security policies that align with the organisation's broader information risk management policies and objectives. Follow recognised network design principles (i.e. ISO/IEC 27033-1:2009) to help define the necessary security qualities for the perimeter and internal network segments and ensure that all network devices are configured to the secure baseline build.

Police the network perimeter: Limit access to network ports, protocols and services and filter and inspect 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 malware and other malicious content:

- **Install firewalls:** Firewalls should be deployed to form a buffer zone between the untrusted external network and the internal network used by the business. The firewall rule set should deny traffic by default and a white list should be applied that only allows authorised protocols and ports to communicate with authorised networks and network addresses. This will reduce the exposure of ICT systems to network based attacks;

- **Prevent malicious content:** Deploy anti-virus and malware checking solutions with heuristic and signature-based capabilities to examine both inbound and outbound data at the perimeter in addition to anti-virus and malware protection deployed on internal networks and on host systems. The anti-virus and malware solutions used at the perimeter should 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 network connectivity between internal systems and systems hosted on untrusted networks (such as the Internet), limit the exposure of sensitive information and monitor network traffic to detect and react to attempted and actual network intrusions.

- **Segregate network assets:** Identify, group and isolate critical business information assets and services and apply appropriate network security controls to them;

- **Secure wireless devices:** Wireless devices should only be allowed to connect to trusted wireless networks. All wireless access points should be secured and security scanning tools should have the ability to detect wireless access points;

- **Protect internal Internet Protocol (IP) addresses:** Implement capabilities (such as Network Address Translation) to prevent internal IP addresses from being exposed to external networks and attackers and ensure that it is not possible to route network traffic directly from untrusted networks to internal networks;

- **Enable secure administration:** Administrator access to any network component should only be carried out over dedicated network infrastructure and secure channels using communication protocols that support encryption;

- **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:** Tools such as network intrusion detection and network intrusion prevention should be placed on the network and configured by qualified staff to monitor traffic for unusual or malicious incoming and outgoing activity that could be indicative of an attack or an attempt. Alerts generated by the system should be promptly managed by appropriately trained staff;

- **Assurance processes:** Conduct regular penetration tests of the network infrastructure and undertake simulated cyber attack exercises to ensure that all security controls have been implemented correctly and are providing the necessary levels of security.

CESG
The Information Security Arm of GCHQ

Managing User Privileges

Summary

It is good practice for an organisation to manage the access privileges that users have to an Information and Communications Technologies (ICT), the information it holds and the services it provides. All users of ICT systems should only be provided with the privileges that they need to do their job. This principle is often referred to as 'Least Privilege'. A failure to manage user privileges appropriately may result in an increase in the number of deliberate and accidental attacks.

What is the risk?

Businesses and organisations should understand what access employees need to information, services and resources in order to do their job. Otherwise they will not be able to grant ICT system rights and permissions to individual users or groups of users that are proportionate to their role within the organisation. Failure to effectively manage user privileges could result in the following risks being realised:

- **Misuse of privileges:** Authorised users can misuse the privileges assigned to them to either deliberately or accidentally compromise ICT systems. For example to make unauthorised changes to the configuration of systems, leading to a loss of the confidentiality, integrity or availability of information or ICT systems;

- **Increased attacker capability:** Attackers will use compromised user accounts to carry out their attacks and, if allowed to, they will return and reuse the compromised account on numerous occasions, or sell the access to others. The system privileges provided to the compromised account will be available to the attacker to use. Ultimately attackers will seek to gain access to root or administrative accounts to allow them full access to all system information, services and resources;

- **Negating established security controls:** Where attackers have privileged access to ICT systems they will attempt to cover their tracks by making changes to security controls or deleting accounting and audit logs so that their activities are not detected.

BIS Department for Business Innovation & Skills
CPNI Centre for the Protection of National Infrastructure
CabinetOffice Office of Cyber Security & Information Assurance

How can the risk be managed?

Businesses and organisations that effectively manage user privileges can limit and control the activities of their users on their ICT systems. Organisations need to determine the system privileges that users need to fulfil their business role, on the basis of 'Least Privilege'.

Establish effective account management processes: Corporate processes and procedures should manage and review user accounts from creation and modification through to eventual deletion when a member of staff leaves. Unused or dormant accounts, perhaps provided for temporary staff or for testing purposes, should be removed or suspended in-line with corporate policy;

Limit the number and use of privileged accounts: Strictly control the number of privileged accounts for roles such as system or database administrators. Ensure that this type of account is not used for high risk or day to day user activities, for example to gain access to external e-mail or browse the Internet. Provide administrators with normal accounts for business use. The requirement to hold a privileged account should be reviewed more frequently than 'standard user' accounts;

Limit user privileges: Users should only be provided with the rights and permissions to systems, services, information and resources that they need to fulfil their business role;

Monitor all users: Monitor user activity, particularly all access to sensitive information and the use of privileged account actions, such as the creation of new user accounts, changes to user passwords or the deletion of accounts and audit logs;

Establish policy and standards for user identification and access control: The quality of user passwords and their lifecycle should be determined by a corporate policy. Ideally they should be machine generated, randomised passwords. If this is not possible, password complexity rules should be enforced by the system. For some ICT systems an additional authentication factor (such as a physical token) may be necessary and this should be identified in the risk assessment. Access controls should be allocated on the basis of business need and 'Least Privilege';

Set up a personnel screening process: All users need to undergo some form of pre-employment screening to a level that is commensurate with the sensitivity of the information they will have access to;

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 and availability of the content and all privileged user access recorded;

Educate users and maintain their awareness: Without exception, all users should be aware of the policy regarding acceptable account usage and their personal responsibility to adhere to corporate security policies and the disciplinary measures that could be applied for failure to do so.

CESG
The Information Security Arm of GCHQ

User Education and Awareness

Summary

Unfortunately the use made by employees of an organisation's Information and Communications Technologies (ICT) brings with it various risks. It is critical for all staff to be aware of their personal security responsibilities and the requirement to comply with corporate security policies. This can be achieved through systematic delivery of a security training and awareness programme that actively seeks to increase the levels of security expertise and knowledge across the organisation as well as a security-conscious culture.

What is the risk?

Organisations that do not produce user security policies or train their users in recognised good security practices will be vulnerable to many of the following risks:

- **Unacceptable use:** Without a clear policy on what is considered to be acceptable, certain actions by users may contravene good security practice and could lead to the compromise of personal or sensitive commercial information that could result in legal or regulatory sanctions and reputational damage;
- **Removable media and personal devices:** Unless it is clearly set out in policy and communicated, staff may consider it acceptable to use their own removable media or connect their personal device to the corporate infrastructure. This could potentially lead to the import of malware and the compromise of personal or sensitive commercial information;
- **Legal and regulatory sanction:** If users are not aware of any special handling or the reporting requirements for particular classes of sensitive information the organisation may be subject to legal and regulatory sanctions;
- **Incident reporting:** If users do not report incidents promptly the impact of any incident could be compounded;
- **Security Operating Procedures:** If users are not trained in the secure use of their organisation's ICT systems or the functions of a security control, they may accidentally misuse the system, potentially compromising a security control and the confidentiality, integrity and availability of the information held on the system;
- **External attack:** Users remain the weakest link in the security chain and they will always be a primary focus for a range of attacks (phishing, social engineering, etc) because, when compared to a technical attack, there is a greater likelihood of success and the attacks are cheaper to mount. In many instances, a successful attack only requires one user to divulge a logon credential or open an email with malicious content;

BIS Department for Business Innovation & Skills
CPNI Centre for the Protection of National Infrastructure
CabinetOffice Office of Cyber Security & Information Assurance

- **Insider threat:** A significant change in an employee's personal situation could make them vulnerable to coercion and they may release personal or sensitive commercial information to others. Dissatisfied users may try to abuse their system level privileges or coerce other users, 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: The organisation should develop and produce a user security policy (as part of their overarching corporate security policy) that covers acceptable use. Security procedures for all ICT systems should be produced that are appropriate and relevant to all business roles;

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 (contracts for contractors and third party users) must be formally acknowledged and retained to support any subsequent disciplinary action. Ideally, the initial user registration process should also be linked to the organisation's technical access controls;

Maintain user awareness of the cyber risks faced by the organisation: Without exception, all users should receive regular refresher training on the cyber risks to the organisation and to them as both employees and individuals;

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

Carry out pre-employment screening: Background security checks that are commensurate with the individual's role, the sensitivity of the information they will access and the organisation's overarching approach to risk management should be carried out and revisited periodically as appropriate. This process may also be applied to all employees, contractors and third party users;

Monitor the effectiveness of security training: Establish mechanisms to test the effectiveness and value of the security training provided to all staff. This should be done through formal feedback and potentially by including questions in the staff survey on security training and the organisation's security culture. Those areas that regularly feature in security reports or achieve the lowest feedback ratings should be targeted for remedial action;

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;

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.

CESG
The Information Security Arm of GCHQ

Incident Management

Summary

All organisations will experience an information security incident 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 reduce any financial impact.

What is the risk?

Security incidents are inevitable and they will range in their business impact. All incidents need to be effectively managed, particularly those that invoke the organisation's disaster recovery and business continuity plans. Some incidents can, on further analysis, be indicative of more severe underlying problems.

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

- **A major disruption of business operations:** Failure to realise that an incident has occurred and manage it effectively may compound the impact of the incident, leading to a long term outage, serious financial loss and erosion of customer confidence;

- **Continual business disruption:** An organisation that fails to address the root cause of incidents by addressing weaknesses in the corporate security architecture could be exposed to consistent and damaging business disruption;

- **Failure to comply with legal and regulatory reporting requirements:** An incident resulting in the compromise of sensitive information covered by mandatory reporting controls that are not adhered to could lead to legal or regulatory penalties.

The organisation's business profile will determine the type and nature of incidents that may occur and so a risk-based approach that considers all business processes should be used to shape the incident management plans. In addition, the quality and effectiveness of the security policies and the standards applied by the organisation will also be contributing factors to preventing incidents.

How can the risk be managed?

Obtain senior management approval and backing: The organisation's Board needs to understand the risks and benefits of incident management, provide appropriate funding to resource it and lead the delivery;

Establish an incident response capability: The organisation should identify the funding and resources to develop, deliver and maintain an organisation-wide incident management capability that can address the full range of incidents that could occur. The supporting policy processes and plans should be risk based and cover any legal and regulatory reporting or data accountability requirements;

BIS Department for Business Innovation & Skills
CPNI Centre for the Protection of National Infrastructure
CabinetOffice Office of Cyber Security & Information Assurance

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. The organisation should identify recognised sources of specialist incident management training and maintain the organisation's skill base;

Define the required roles and responsibilities: The organisation needs to appoint and empower specific individuals to handle ICT incidents and provide them with clear terms of reference to manage any type of incident that may occur;

Establish a data recovery capability: Data losses occur and so a systematic approach to the backup of the corporate information asset base should be implemented. Backup media should be held in a physically secure location on-site and off-site where at all possible and 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 Disaster Recover and Business Continuity) should be regularly tested. The outcome of the tests should be used to inform the development and gauge the effectiveness of the incident management plans;

Decide what information will be shared and with whom: For information bound by specific legal and regulatory requirements the organisation may have to report any incidents that affect the status of that information within a specific time-frame. All internal and external reporting requirements should be clearly identified in the Incident Management Plans;

Collect and analyse post-incident evidence: The preservation and analysis of the user or network activity that led up to the event is critical to identify and remedy the root cause of an incident. The collected evidence could potentially support any follow on disciplinary or legal action and the incident management policy needs to set out clear guidelines to follow that comply with a recognised code of practice;

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 related security policy, process or user training that could have prevented the incident from occurring;

Educate users and maintain their awareness: All users should be made aware of their responsibilities and the procedures they should follow to report and respond to an incident. Equally, all users should be encouraged to report any security weaknesses or incident as soon as possible and without fear of recrimination;

Report criminal incidents to Law Enforcement: It is important that online crimes are reported to Action Fraud or the relevant law enforcement agency to build a clearer view of the national threat picture and deliver an appropriate response.

CESG
The Information Security Arm of GCHQ

Malware Prevention

Summary

Any information exchange carries a degree of risk as it could expose the organisation to malicious code and content (malware) which could seriously damage the confidentiality, integrity and availability of the organisation's information and Information and Communications Technologies (ICT) on which it is hosted. The risk may be reduced by implementing security controls to manage the risks to all business activities.

What is the risk?

Malware infections can result in the disruption of business services, the unauthorised export of sensitive information, material financial loss and legal or regulatory sanctions. The range, volume and originators of information exchanged with the business and the technologies that support them provide a range of opportunities for malware to be imported. Examples include:

- **E-mail:** Still provides the primary path for internal and external information exchange. It can be used for targeted or random attacks (phishing) through malicious file attachments that will release their payload when the file is opened or contain embedded links that redirect the recipient to a website that then downloads malicious content;

- **Web browsing and access to social media:** Uncontrolled browsing and access to social media web sites and applications could provide an opportunity for an attacker to direct malicious content to a individual user or lead to the download of malicious content from a compromised or malicious web site;

- **Removable media and personal devices:** Malware can be transferred to a corporate ICT system through the use of unapproved media or the initial connection of a personal device.

How can the risk be managed?

Develop and publish corporate policies: Develop and implement policies, standards and processes that deliver the overall risk management objectives but directly address the business processes that are vulnerable to malware;

Establish anti-malware defences across the organisation: Agree a top level corporate approach to managing the risk from malware that is applicable and relevant to all business areas;

Scan for malware across the organisation: Protect all host and client machines with anti-virus solutions that will actively scan for malware;

Manage all data import and export: All information supplied to or from the organisation electronically should be scanned for malicious content;

BIS Department for Business Innovation & Skills
CPNI Centre for the Protection of National Infrastructure
CabinetOffice Office of Cyber Security & Information Assurance

Blacklist malicious web sites: Ensure that the perimeter gateway uses blacklisting to block access to known malicious web sites;

Provide dedicated media scanning machines: Stand-alone workstations (with no network connectivity) should be provided and equipped with two Anti-Virus products. The workstation should be capable of scanning the content contained on any type of media and, ideally, every scan should be traceable to an individual;

Establish malware defences: Malware can attack any system process or function so the adoption of security architecture principles that provide multiple defensive layers (Defence in Depth) should be considered. The following controls are considered essential to manage the risks from malware:

- Deploy Anti-Virus and malicious code checking solutions with heuristic and signature-based capabilities to continuously scan inbound and outbound objects at the perimeter, on internal networks and on host systems, preferably using different products at each layer. This will increase detection capabilities whilst reducing risks posed by any deficiencies in individual products. Any suspicious or infected 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 the common desktop applications used by the user, the web browser being a prime example. Content filtering can also help to counter the risks from a compromised information release mechanism or authorisation process that may allow sensitive data to be sent to external networks;

- Install firewalls on the host and gateway devices and configure them to deny traffic by default, allowing only connectivity associated with known white listed applications;

- If the business processes can support it, disable Windows Scripting, Active X, VBScript and JavaScript;

- Where possible, disable the auto run function to prevent the automatic import of malicious code from any type of removable media. Equally, if removable media is introduced, the system should automatically scan it for malicious content;

- Regularly scan every network component and apply security patches in compliance with the corporate security patching and vulnerability management policy;

- Apply the secure baseline build to every network device and mobile platform.

User education and awareness: Users should understand the risks from malware and the day to day secure processes they need to follow to prevent a malware infection from occurring. The security operating procedures for the corporate desktop should contain the following:

- Comply with the removable media policy at all times;
- Do not open attachments from unsolicited e-mails;
- Do not click on hyperlinks in unsolicited e-mails;
- Do not connect any removable media received as a gift to the corporate network;
- Do not connect any unapproved personal device to the corporate network;
- Report any strange or unexpected system behaviours to the appropriate security team;
- Maintain an awareness of how to report a security incident.

CESG
The Information Security Arm of GCHQ

Monitoring

Summary

Monitoring Information and Communications Technologies (ICT) activity allows businesses to detect attacks and react to them appropriately whilst providing a basis upon which lessons can be learned to improve the overall security of the business. In addition, monitoring the use of ICT systems allows the business to ensure that systems are being used appropriately in accordance with organisational policies. Monitoring is often a key capability needed to comply with security, legal and regulatory requirements.

What is the risk?

Monitoring the organisation's ICT systems provides the business with the means to assess how they are being used by authorised users and if they have been or are being attacked. Without the ability to monitor, an organisation will not be able to:

- **Detect attacks:** Either originating from outside the organisation or attacks as a result of deliberate or accidental insider activity;
- **React to attacks:** So that an appropriate and proportionate response can be taken to prevent or minimise the resultant impact of an attack on the business;
- **Account for activity:** The business will not have a complete understanding of how their ICT systems or information assets are being used or enforce user accountability.

Failure to monitor ICT systems and their use for specific business processes could lead to non-compliance with the corporate security policy and legal or regulatory requirements or result in attacks going unnoticed.

How can the risk be managed?

Businesses need to put strategies, policies, systems and processes in place to ensure that they are capable of monitoring their ICT systems and respond appropriately to attacks. A consistent approach to monitoring needs to be adopted across the business that is based on a clear understanding of the risks.

Establish a monitoring strategy and supporting policies: Develop and implement an organisational monitoring strategy and policy based on an assessment of the risks. The strategy should take into account any previous security incidents and attacks and align with the organisation's incident management policies;

BIS Department for Business Innovation & Skills
CPNI Centre for the Protection of National Infrastructure
CabinetOffice Office of Cyber Security & Information Assurance

Monitor all ICT systems: Ensure that the solution monitors all networks and host systems (such as clients and servers) potentially through the use of Network and Host Intrusion Detection Systems (NIDS/HIDS) and Prevention Solutions (NIPS/HIPS), supplemented as required by Wireless Intrusion Detection Systems (WIDS) that work in harmony with the wired IDS. These solutions should provide both signature based capabilities to detect known attacks and heuristic capabilities to detect potentially unknown attacks through new or unusual system behaviour;

Monitor network traffic: The inbound and outbound network traffic traversing network boundaries should be continuously monitored to identify unusual activity or trends that could indicate attacks and the compromise of data. The transfer of sensitive information, particularly large data transfers or unauthorised encrypted traffic should automatically generate a security alert and prompt a follow up investigation. The analysis of network traffic can be a key tool in preventing the loss of data;

Monitor all user activity: The monitoring capability should have the ability to generate audit logs that are capable of identifying unauthorised or accidental input, misuse of technology or data. Critically, it should be able to identify the user, the activity that prompted the alert and the information they were attempting to access;

Test legal compliance: Ensure that the monitoring processes comply with legal or regulatory constraints on the monitoring of user activity;

Fine-tune monitoring systems: Ensure that monitoring systems are fine-tuned appropriately only to collect logs, events and alerts that are relevant in the context of delivering the requirements of the monitoring policy. Inappropriate collection of monitoring information could breach data protection and privacy legislation. It could also be costly in terms storing the audit information and could hinder the efficient detection of real attacks;

Establish a centralised collection and analysis capability: Develop and deploy a centralised capability that can collect and analyse accounting logs and security alerts from ICT systems across the organisation, including user systems, servers, network devices, and including security appliances, systems and applications. Ensure that the design and implementation of the centralised solution does not provide an opportunity for attackers to bypass normal network security and access controls;

Ensure there is sufficient storage: Security managers should determine the types of information needed to satisfy the organisation's monitoring policy. Vast quantities of data can be generated and appropriate storage will need to be made available. The organisation will also need to consider the sensitivity of the processed audit logs and any requirement for archiving to satisfy any regulatory or legal requirements;

Provide two synchronised timing sources: 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 time-stamp audit logs, alerts and events to support incident response, security investigations and disciplinary or legal action;

Train the security personnel: Ensure that security personnel receive appropriate training on the deployment of monitoring capability and the analysis of security alerts, events and accounting logs;

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 and learn from security incidents and improve the efficiency of the monitoring capability.

CESG
The Information Security Arm of GCHQ

Removable Media Controls

Summary

Failure to control or manage the use of removable media can lead to material financial loss, the theft of information, the introduction of malware and the erosion of business reputation. It is good practice to carry out a risk benefit analysis of the use of removable media and apply appropriate and proportionate security controls, in the context of their business and risk appetite.

What is the risk?

The use of removable media to store or transfer significant amounts of personal and commercially sensitive information is an everyday business process. However, if organisations fail to control and manage the import and export of information from their Information and Communications Technologies (ICT) using removable media they could be exposed to the following risks:

- **Loss of information:** The physical design of removable media can result in it being misplaced or stolen, potentially compromising the confidentiality and availability of the information stored on it;
- **Introduction of malware:** The uncontrolled use of removable media will increase the risk from malware if the media can be used on multiple ICT systems;
- **Information leakage:** Some media types retain information after user deletion, this could lead to an unauthorised transfer of information between systems;
- **Reputational damage:** A loss of sensitive data often attracts media attention which could erode customer confidence in the business;
- **Financial loss:** If sensitive information is lost or compromised the organisation could be subjected to financial penalties.

How can the risk be managed?

Removable media should only be used to store or transfer information as a last resort, under normal circumstances information should be stored on corporate systems and exchanged using appropriately protected and approved information exchange connections.

Produce corporate policies: Develop and implement policies, processes and solutions to control the use of removable media for the import and export of information;

Limit the use of removable media: Where the use of removable media is unavoidable the business should limit the media types that can be used together with the users, systems and types of information that can be stored or transferred on removable media;

BIS Department for Business Innovation & Skills
CPNI Centre for the Protection of National Infrastructure
CabinetOffice Office of Cyber Security & Information Assurance

Scan all media for malware: Protect all host systems (clients and servers) with an anti-virus solution that will actively scan for malware when any type of removable media is introduced. The removable media policy should also ensure that any media brought into the organisation is scanned for malicious content by a standalone media scanner before any data transfer takes place;

Audit media holdings regularly: All removable media should be formally issued by the organisation to individuals who will be accountable for its secure use and return for destruction or reuse. Records of holdings and use should be made available for audit purposes;

Encrypt the information held on the media: Where removable media has to be used, the information should be encrypted. The type of encryption should be proportionate to the value of the information and the risks posed to it;

Lock down access to media drives: The secure baseline build should deny access to media drives (including USB drives) by default and only allow access to approved authorised devices;

Monitor systems: The monitoring strategy should include the capability to detect and react to the unauthorised use of removable media within an acceptable time frame;

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 approved overwriting process to the physical destruction of the media by an approved third party;

Educate users and maintain their awareness: Ensure that all users are aware of the risks posed to the organisation from the use of removable media and their personal security responsibility for following the corporate removable media security policy.

CESG
The Information Security Arm of GCHQ

Home and Mobile Working

Summary

Mobile working offers great business benefit but exposes the organisation to risks that will be challenging to manage. Mobile working extends the corporate security boundary to the user's location. It is advisable for organisations to establish risk-based policies and procedures that cover all types of mobile devices and flexible working if they are to effectively manage the risks. Organisations should also plan for an increase in the number of security incidents and have a strategy in place to manage the loss or compromise of personal and commercially sensitive information and any legal, regulatory or reputational impact that may result.

What is the risk?

Mobile working entails the transit and storage of information assets outside the secure corporate infrastructure, probably across the Internet to devices that may have limited security features. Mobile devices are used in public spaces where there is the risk of oversight and they are also highly vulnerable to theft and loss.

If the organisation does not follow good practice security principles and security policies the following risks could be realised:

- **Loss or theft of the device:** Mobile devices are highly vulnerable to being lost or stolen because they are attractive and valuable devices. They are often used in open view in locations that cannot offer the same level of physical security as the organisation's own premises;
- **Being overlooked:** Some users will have to work in public open spaces where they are vulnerable to being observed when working on their mobile device, potentially compromising personal or sensitive commercial information or their user credentials;
- **Loss of credentials:** If user credentials (such as username, password, token) are stored with a device used for remote working and it is lost or stolen, the attacker could potentially compromise the confidentiality, integrity and availability of the organisation's Information and Communications Technologies (ICT);
- **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 mobile device that could result in the compromise of the confidentiality or integrity of the information;

BIS Department for Business Innovation & Skills
CPNI Centre for the Protection of National Infrastructure
CabinetOffice Office of Cyber Security & Information Assurance

- **Compromise of the secure configuration:** Without correct training a user may accidentally or intentionally remove or reconfigure a security enforcing control on the mobile device and compromise the secure configuration. This could expose the device to a range of logical attacks that could result in the compromise or loss of any personal or sensitive commercial information the device is storing.

How can the risk be managed?

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

Educate users and maintain their awareness: Without exception, all users should be trained on the secure use of their mobile device for the locations they will be working in. Users should be capable of operating the device securely by following their user specific security procedures at all times, which should as a minimum include direction on:

- Secure storage and management of their user credentials;
- Incident reporting;
- Environmental awareness (the risks from being overlooked etc).

Apply the secure baseline build: All ICT systems should be configured to the secure baseline build including all types of mobile device used by the organisation;

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 when working 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 an untrusted public network such as the Internet. The device and the information exchange should be protected by an appropriately configured Virtual Private Network (VPN);

Review the corporate incident management plans: Mobile working attracts significant risks and security incidents will occur even when users follow the security procedures (such as a forced attack where the user is physically attacked to gain control of the device). The corporate 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 in international locations. 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.