National Cyber Security Centre
a part of GCHQ

CPNI
Centre for the Protection of National Infrastructure

Reducing data exfiltration by malicious insiders

Advice and recommendations for mitigating this type of insider behaviour.

About this guidance

This guidance can help organisations to reduce the likelihood of data exfiltration by malicious insiders. It's aimed at staff responsible for delivering insider risk mitigation programmes, including technical leaders, business delivery owners, senior line managers, and staff working in HR, data protection and legal departments.

This guidance provides **examples** of the methods malicious insiders have used or could use to exfiltrate data, and suggests technical measures that can be used to:

- **prevent** data exfiltration
- enable **monitoring**
- carry out post-event **audit**

Note:

Mitigations for data exfiltration should be one element within an overall framework of insider risk mitigation. This guidance assumes that organisations already have in place such a framework (such as **CPNI's Insider Risk Mitigation Framework**), and also procedures in place for managing incident response following data exfiltration (see NCSC's guidance on **managing cyber incidents**)

In this guidance

Introduction

Malicious insider activity is relatively rare, but can have a major impact on an organisation when it does occur. It is defined as when anyone who has legitimate access to your organisation's assets exploits their position for unauthorised purposes (so not just employees, but also contractors, partners and suppliers).

The majority of insider breaches are not malicious, but are a result of staff performing their daily roles which can be made harder than necessary due to restrictive security. For example, consider a member of staff who has written their passwords on a post-it note under their keyboard because they have to enter five long, complex passwords to access the required systems. For instances such as this, it is important to distinguish between staff who adopt insecure workarounds because security policies conflict with business requirements, and staff who are genuinely malicious insiders.

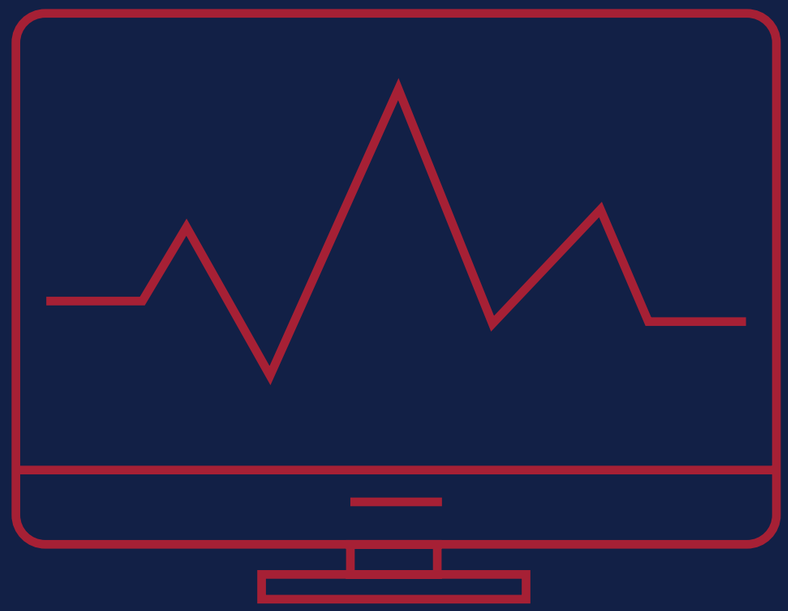
Your organisational risk mitigation decisions should be based upon achieving a balance between business delivery needs, policies and technical controls. Mitigations for data exfiltration should be understood by all employees, embedded in relevant policies, and supported by the organisation's security culture.

Prevent, monitor, audit

The measures you take to **prevent**, **monitor** or retrospectively **audit** data exfiltration by malicious insiders can also reduce the risk of data breaches by your staff. The measures will also provide some protection against data exfiltration by external attackers who have penetrated the organisation's network, or captured and exploited valid credentials.

Note that:

- You will need to interpret this guidance according to your organisation's own circumstances. This includes your use of trusted service providers, future technology developments, acquisitions, mergers and divestitures, and upgrades or modifications to existing technologies.
- You should already have appropriate governance of **insider risk mitigation**, and have carried out essential activities including identifying critical assets. Without these it is difficult for organisations to make informed decisions about balancing technical controls with business processes, which is necessary for continued productivity.



Technical measures that can prevent data exfiltration

The technical controls to mitigate the risk of data exfiltration is founded on 3 elements:

1. Prevent

With careful consideration to business delivery and processes, organisations should put mitigations in place to **prevent data exfiltration or limit access to sensitive data in terms of least privilege**. Where there is legitimate need, this should be carefully monitored, with an easy way for administrators to manage access controls as employees change roles, and their needs alter. Refer to the NCSC's **Cyber Security Design Principles** for advice about how to make compromise difficult.

Controlling the use of external storage devices is a major step in mitigating data exfiltration. More information on how to manage this can be found in the NCSC's **Device Security Principles**. Clear communication of why necessary controls exist can reduce staff frustration at workflow impacts, especially where there is also realistic ability to **perform tasks in line with policy**. If prevention is not possible or desirable then the next step is monitoring.

2. Monitor

Monitoring may have several purposes including:

- near real-time monitoring to give the user a warning that their action may be risky or breaching policy (for example, a pop-up message warning that an email address is outside the organisation)
- near real time monitoring that allows the organisation to quarantine an action pending human intervention (for example, sending OFFICIAL SENSITIVE material from a government department to an email address that is not @gov.uk)
- post-event monitoring that allows the organisation to identify trends at an individual or group level that may need interventions in order to protect security
- enhanced monitoring for privileged users (often seen as a 'badge of honour' within organisations)

Where prevention is not suitable, organisations will want to monitor user activity in a way that is both **legal and proportionate**. Given the potential volume of data that can be collected, it is useful to have the ability to fine tune monitoring so that it focuses on critical assets, on users of concern (those who have been flagged for enhanced monitoring, e.g. for behaviours or JML process) and on privileged users. Email is a particularly common method for data exfiltration, effective monitoring of email traffic can provide significant mitigations.

A level of staff awareness about the existence of security monitoring is important, with purposes laid out in clear and accessible IT use policies. Staff acceptance of monitoring is more likely when:

- the **organisational culture is positive** and security monitoring is considered usual practice
- the data is not abused or used beyond the purposes explained to staff

Reminders of the presence of security monitoring can be beneficial in discouraging individuals from malicious insider activity. Since most policy breaches are non-malicious, we recommend you take a constructive approach. This might start with "We've noticed you trying to do '*ABC*', which is unsecure for '*XYZ*'. What issue are you dealing with and how can we help you in resolving it?".

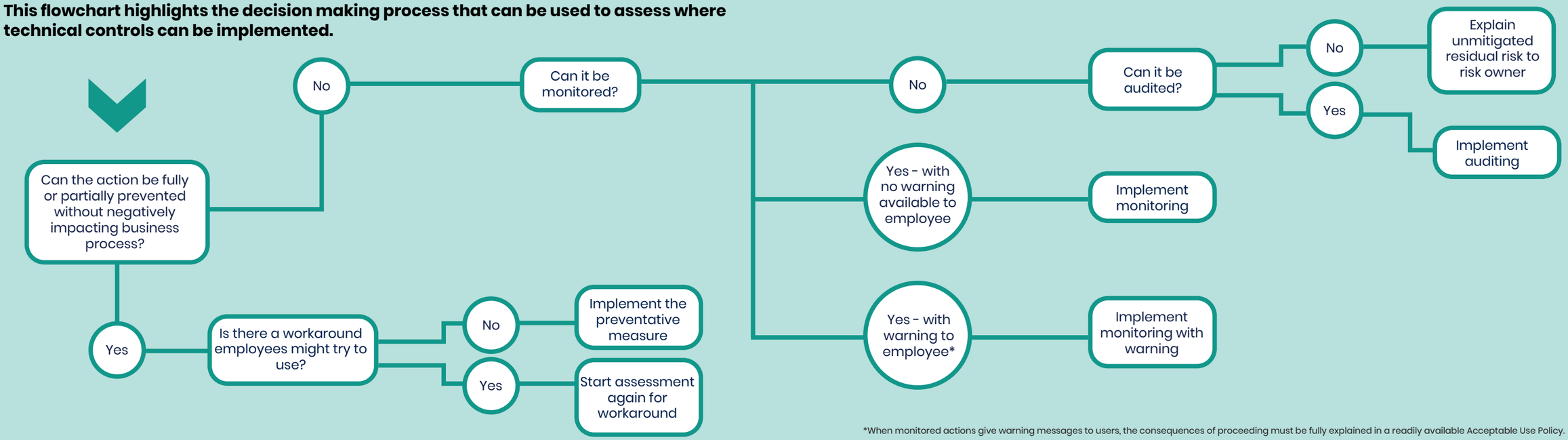
3. Audit

Irrespective of the prevention and active monitoring controls deployed, organisations need the capability to audit to capture post-event activity relating to users, data, and assets. Auditing effectively provides a backstop when prevention and monitoring are not possible.

Due consideration should be given to who has **access to activity logs and ability to edit them** to keep them secure from tampering. Malicious insiders can include long-serving employees with good working knowledge of the organisation's systems. Security monitoring and logging is an in-depth topic, more detailed information on setting it up can be found in the **relevant NCSC guidance**.

Technical measures that can prevent data exfiltration

This flowchart highlights the decision making process that can be used to assess where technical controls can be implemented.



*When monitored actions give warning messages to users, the consequences of proceeding must be fully explained in a readily available Acceptable Use Policy.

Technical controls

Technical controls to **Prevent, Monitor and Audit** need to be applicable across the organisation's entire estate including BYOD, contractors and remote/home working where applicable. The rise in **home working** and **Bring Your Own Device** solutions provide many benefits to an organisation but also introduce a number of challenges for security, including risks of data exfiltration.

Technical controls for consideration include:

- implementation of rules within products, apps and services
- deny listing/allow listing (by URL, IP ranges, applications, protocols, bi/dual directional rules etc)
- preventing use of steganography applications
- preventing or controlling the use of translation sites
- endpoint/mobile device management
- mobile application management
- data loss prevention software (including content inspection)
- security incident event management (SIEM) solutions
- log management and analysis
- controlling use of external storage devices
- controlling for abuse of email

The appropriate mitigation measures to take will vary according to the situation, as risks will be different for different users. For example, enhancing monitoring of employees in the 30 days before they leave and/or as soon as they have given notice, or when they are advised they are in scope of possible redundancy. In this case, ensure the recovery of official devices and closing of accounts when they leave, including consideration of BYOD solutions. It may be appropriate to conduct a rigorous post-departure audit of their activities on the network in the relevant period before their departure. In other situations, enhanced monitoring could be mandatory for the job role, or BYOD judged too high-risk for the activity.

Recommended mitigations for data exfiltration

Achieving an appropriate balance between risk mitigation, business efficiency and organisational/security cultures is a challenge for all organisations. It can only be achieved through a healthy discussion between technical leads, business delivery leads and risk owners. This must be conducted as part of an overall insider risk mitigation programme, with sound governance and clear understanding of the board's appetite for risk.

The following recommendations (which are not exhaustive) will help your organisation achieve the right balance:

1. Baseline what measures are already in place to **Prevent**, **Monitor** and **Audit** the common methods of data exfiltration, and assess the residual risk to the organisation's critical information assets. **Appendix A** will help with this.

2. Ensure that best use is being made of existing tools before investing in new ones. Identify what can be improved, not just from a *technical* perspective, but also in terms of *process* (for example, implementing a thorough joiners/movers/leavers procedure). Using **Appendix A** can assist the business case for any new investment.

3. Recognise where existing security policies (such as **enforcing arbitrary password complexity requirements**) conflict with the ability of users to go about their day-to-day tasks. Work with staff to understand issues and co-create policy & processes to satisfy both security and usability.

4. Ensure that change management protocols are in place to check that neither technology changes nor business delivery developments (including organisational change) can take place without prior assessment of the security risks. This should specifically include any changes to your vulnerability to data exfiltration by malicious insiders.

5. Adopt a flexible approach to preventative measures, especially monitoring. Good practice guidance on employee monitoring is that it must be proportionate and locally lawful. It should not be conducted covertly or individually targeted. Therefore, with regard to data exfiltration prevention, the strictest controls should be applied to high risk users and to critical assets.

6. Give careful consideration to the proportionate protective measures around those who work part time for your organisation and part time for others including 'Need to Know' access only as required for their role. This may include senior people such as non-executive directors as well as consultants and contractors. If they have multiple accounts (including yours) on their devices, consider protective measures that prevent data leakage from your network to others.

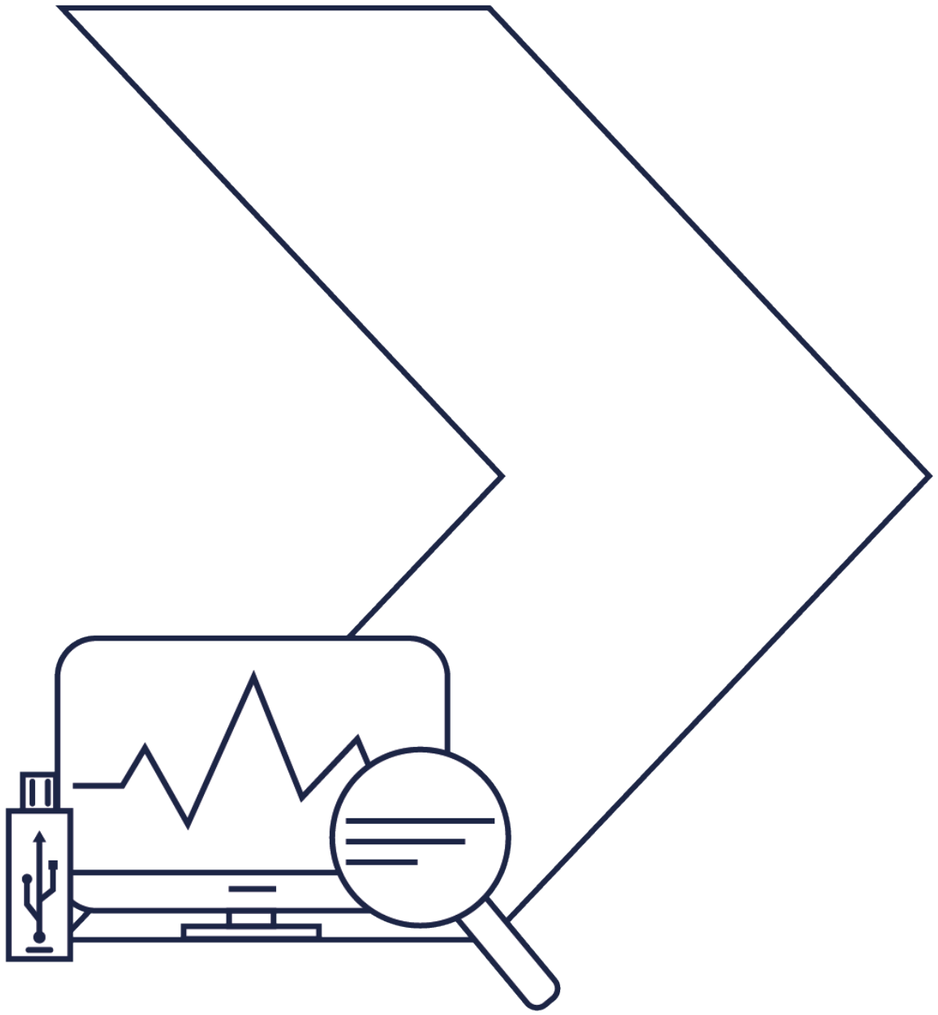
This guidance has been collaboratively produced by CPNI, NCSC and SITIIE (Securing IT against Insiders Information Exchange).

Appendix A:
Baseline assessment of exfiltration techniques

Baseline assessment of exfiltration techniques

This table can be completed by organisations to prepare a baseline assessment of their critical assets, adding additional lines if necessary (and ignoring those that are not relevant). This process should be seen as part of the organisation's overall security risk management process. Once completed, organisations should review relevant policies in case of necessary updates.

Columns **2** and **3** should normally be completed by technical leads to inform a subsequent conversation with business leads and risk owners (who would normally complete columns **4** and **5**).



1 **Method**	2 **Current state (prevent/ monitor/audit)**	3 **Residual risk**	4 **Technology to upgrade without impacting business delivery (and cost)**	5 **Residual risk after upgrade**
Obfuscation/ Steganography				
Copy and paste				
Screen grab and paste				
Save data with new name				
Save data in different file format				
Save data with protective marking removed				
Translate				
Shrink file and embed in another document				
Steganography within .jpeg				
Use of private/medical/personal filesnames				
Exfiltration				
Email				
Webmail				
External storage devices				
Secure messaging platforms				
Online conference facilities				
Social media				
Wi-Fi/Bluetooth				
Multiple accounts on single device				

Appendix B:
Why and how is data exfiltrated?

Why and how is data exfiltrated?

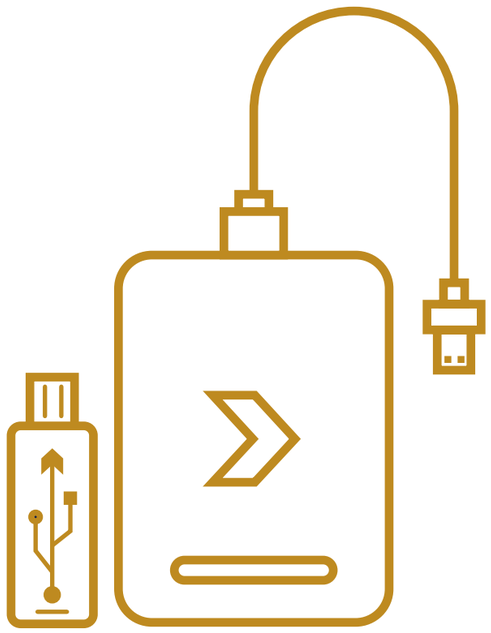
Data exfiltration predates the digital age, and physical methods of data exfiltration are still used (such as photographing computer screens, and stealing un-shredded classified waste). However, even physical exfiltration methods will link back to data contained in digital records, as will information that is orally passed by insiders to external bodies.

Malicious insiders exfiltrate data for a variety of reasons, including:

- personal gain (such as stealing data for use in a future employment)
- revenge (staff may feel wronged, unrewarded, or unrecognised)
- ideology, belief or political allegiance (such as leaking controversial policies to the media)
- ego (staff may feel a sense of personal ownership of data/code developed on behalf of their employer)
- data hoarding (note that many staff save emails and documents they consider to be useful, for non-malicious reasons)
- facilitation of terrorism, crime or espionage (such as stealing details of security systems or intellectual property)
- coercion (via blackmail or extortion, for example)

The method used by the malicious insider will depend on a number of factors, including:

- their risk appetite
- their length of service (longer serving employees are probably better at hiding suspicious activity)
- the degree of help received from external contacts
- their technical competence (privileged IT users may use sophisticated techniques, or may not be subject to the same controls)
- the corporate and personal technology available to the insider (for example, BYOD and remote/home working having greatly increased the opportunities for data exfiltration)



Exfiltration methods

The case studies in **Appendix C** suggest that giving priority to controlling **abuse of email** and **external storage devices** as a matter of priority should help organisations significantly mitigate risk. However, exfiltration of data can be carried out using a wide range of methodologies, listed below.

- email to various addresses (including personal address, fake addresses, friends and family, official/non-official, media, gmail/Hotmail)
- webmail or internet accessible online tools with an upload facility (including use as dead letter box, use of fake addresses)
- external storage devices (including USB, external hard drives, mini and micro SD cards)
- secure messaging platforms (WhatsApp, Signal, Telegram) and apps (Silent Circles)
- online conference facilities (Skype, MS Teams, Zoom) to connect with others including alternate personal addresses
- social media (Facebook, Twitter, Snapchat, Instagram, LinkedIn)
- WiFi/Bluetooth connections to other devices
- multiple accounts on one device or service (senior people, contractors who have multiple employments)

Obfuscation techniques

Before exfiltrating data, the insider may take measures to attempt to conceal their activities through obfuscation and/or steganography (hiding secret data within an ordinary, non-secret, file or message in order to avoid detection). These measures can include, for example:

- copying portions of text (rather than the whole text) and pasting to a new document or application
- screen grabbing/print screen and saving to a new document or application
- saving data with different names and in different file formats
- translating text (via online translation site) to a different language
- shrinking (eg .pdf file or .jpeg image) and pasting into an innocuous document so that it is not visible to visual inspection
- steganography within .jpeg images

Appendix C:
Case Studies

Case studies

Edward Snowden. In 2013 Snowden was a technology contractor working in the US National Security Agency (NSA) outpost in Hawaii. He travelled to Hong Kong with reportedly 1.7 million documents stolen from the NSA, 200,000 of which he handed over to investigative journalists almost immediately. Snowdon was a user with highly privileged access. He extended that access through social engineering. When his downloading activities attracted attention he convinced colleagues that his activities were part of his job, exploiting procedural differences in Hawaii because of its outpost status. Some reports suggest that he copied his data to flash drives that he smuggled past the guards. Another theory is that Snowden used Command and Control servers to receive encrypted data sessions, authenticating them with self-signed certificates.

An employee of a UK government agency, between September 2007 and May 2009, legitimately accessed a number of SECRET and TOP SECRET files relating to the work of UK intelligence agencies. He burned copies of the files to DVD and CD which he physically removed, unchecked, from his place of work. He was arrested in August 2009 when he tried to sell them to the Dutch Secret Intelligence Service. Protective monitoring on all IT accounts (particularly those with access to critical assets), rigorous control of removable media and unpredictable entry and exit searches would mitigate this data exfiltration method.

General David Petraeus. Petraeus resigned as Director of the CIA on 9 November 2012 having had an extra marital affair with his biographer and with whom he improperly shared classified documents. This CIA data breach included the use of online tradecraft involving fake webmail accounts. On the one hand this showed that he knew that what he was doing was improper, but the data transfers were also unencrypted which showed that he was either reckless or incompetent. It is not known what monitoring was applied by CIA to Petraeus but seniority should not be a reason for exemption, especially in the case of seniors with access to critical assets (as is often the case). On 23 April 2015 he pleaded guilty to a single charge of unauthorised removal and retention of classified documents, and was sentenced to 2 years' probation and $100,000 fine.

A disgruntled employee of a large high street supermarket, deliberately made public the salary information of thousands of employees in 2014. He extracted the information via USB stick. Although he had legitimate access to the information, there were no copying or export controls. He made the disclosure at home using a mobile phone, a fake email address and TOR. The impact was significant, including £2.26m in incident response costs, and the case whether the employer had provided suitable safeguards ended up in the UK Supreme Court.

Chelsea Manning. While stationed in Iraq in 2010, Manning, a junior intelligence analyst, passed hundreds of thousands of battlefield reports and diplomatic cables to Wikileaks. Manning had created a computer programme to download a large number of files automatically from State and Defense Department databases. Users at the base were also able to download music and computer games and burn them to CD on the same machines that they used for work. Manning was able to transfer the files by CD to a personal laptop and thence to an SD card for concealed transfer to the US in a camera.

A UK government department leak: An unidentified member of staff leaked a policy draft document to a UK national newspaper. The exfiltration method was almost certainly via WhatsApp on their office mobile (which was also used for managing official emails). The department promoted the use of WhatsApp as a secure messaging means but instigated no controls, such as compartmentalisation of mobiles or monitoring/logging endpoints. The investigation involved up to 180 people having had access to the draft in a very short period of time due to shared mailboxes. Strict 'Need to know' measures would have minimised the number of potential leakers, and use of watermarking technologies increased the chances of identification.

US aerospace engineer steals data from his employer. In 2017 an engineer who had worked for the aerospace company for 16 years, was imprisoned for attempting to sell sensitive information on US military satellites to Russia. The engineer used USB downloads to steal proprietary trade secrets and other technical data from company IT systems. As well as conducting protective monitoring on all IT accounts, an organisation can reduce the risk of sensitive material being removed by restricting access to critical assets, closing USB ports, increasing unpredictable exit searches, and ensuring their guard force is appropriately trained and motivated.

Employee sells corporate data. The data was collated in the employee's draft e-mails under disguised subject headers and was exfiltrated to her contact in 734 WhatsApp messages (subsequently deleted) over a six month period.

A large organisation suffered the leakage of sensitive information to the media, provided as internal communication. Attempts to track email distribution were constrained due to different legalisation between jurisdictions. The same organisation faced challenges in retrieving company IT assets. Often staff, particularly contractors, returned to their native counties with corporate IT. Although their accounts should have been locked once IT received notification of their leaving, the assets often contain sensitive information on their local drives. Some contractors considered they owned the IP of work they may have developed whilst supporting the organisation, due to unclear or ignorance to the engagement contract. Controls implemented were geographical limiting IP address ranges, enhancement of JML process making managers responsible for the recovery of assets, media controls and use of encryption of all information (so if exported, difficult to decrypt) as part of a wider DLP solution. They also now provide a process to allow departing staff to legitimately export personal information.

An organisation discovered very sensitive IP had been hidden within photographs (including personal holiday snaps) and PDFs. When reviewing export controls, it's necessary to ensure suitable technical tools are in place to search for such exfiltration methods, depending upon what applications are permitted on the system in the first place, and the impact of such lost data.

An international organisation undergoing a re-structuring/redundancy programme suffered adverse media attention caused by its staff consultation being made public via MS Teams. Subsequent investigation identified that the meeting invitation had been forwarded directly to the media, but its wider circulation made identification by whom impractical. Subsequently all such invitations contain a traceable unique identifier and a legal confidentially statement is referenced at the beginning of the presentation. It was also identified that documents used within MS Teams presentations were also automatically loaded into OneDrive. Organisations should consider reviewing access control permissions from default of all who are invited to a given meeting.

An organisation's head of sales left the company for a similar role with a competitor, despite the individual's employment contract containing certain constraints. Subsequent check of the individual's account identified they had downloaded sensitive IP, sales contacts and future portfolio information to an unauthorised USB connected device. The individual had also searched the organisation's wider resources and emailed 'internal only' information to their private email address. The lessons identified was whether the employment contract constraints were legally enforceable and whether the organisation was willing to go to court. Alternative remedies used were gaining a legally binding commitment from the individual that they had deleted the information illegally obtained and a legal letter to their new employer warning that should they make any use of the illegally obtained information, legal action would be considered.

Other relevant guidance

Other relevant guidance

NCSC guidance

Cyber Security Design Principles

Cloud Security Guidance

Secure System Administration

Mobile Device Guidance

Growing positive security culture

Security breaches as communication: what are your users telling you?

10 Steps to Cyber Security

Bring Your Own Device

Secure Remote Access

Risk Management for Cyber Security

Password Policy: Updating Your Approach

CPNI guidance

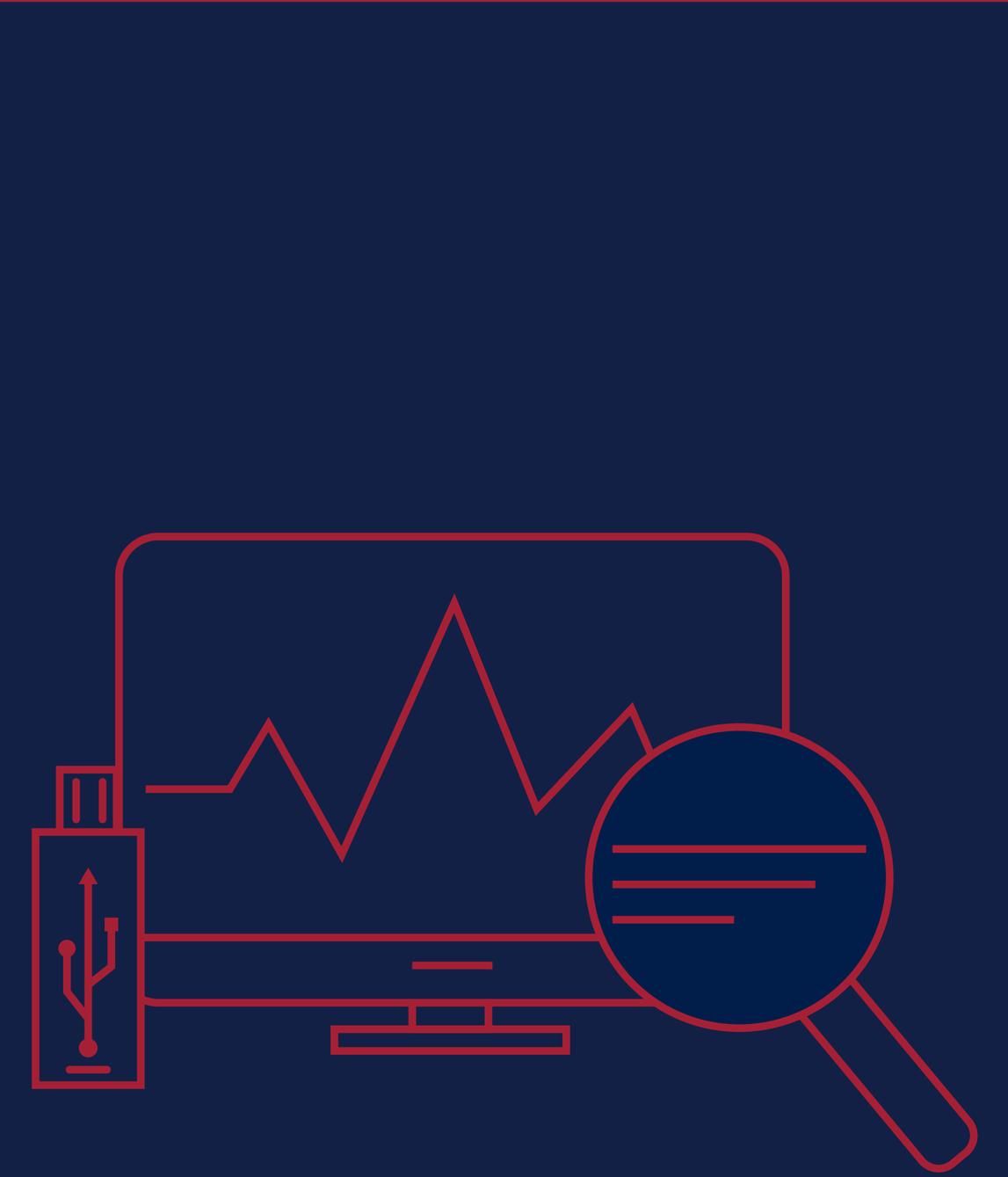
Insider Threat Data Collection Study Report (PDF)

Remote Working Guidance (PDF)

Holistic Management of Employee Risk (HoMER) (PDF)

Exit Procedures (PDF)

Legal Considerations for Employee Monitoring



National Cyber Security Centre
a part of GCHQ

CPNI
Centre for the Protection of National Infrastructure

Disclaimer

The information contained in this document is accurate as at the date it was created. It is intended as general guidance only and you should not rely on it. This information should be adapted for use in the specific circumstances required and you should seek specialist independent professional advice where appropriate before taking any action based on it. To the fullest extent permitted by law, CPNI accept no liability whatsoever for any loss or damage incurred or arising as a result of any error or omission in the guidance or arising from any person acting, relying upon or otherwise using the guidance. Full terms and conditions governing the use of this guidance are available on our website at www.cpni.gov.uk.

Freedom of Information Act (FOIA)

This information is supplied in confidence to the named reader and may not be disclosed further without prior approval from CPNI. This information is exempt from disclosure under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation.