INFS 5115 Security Principles

Insider Attacks

University of South Australia

School of Information Technology and Mathematical Sciences

Insider Attacks

- In this module, we will review the topic of insider attacks.
- We will define these types of threats and discuss their prevalence within the broader threat landscape.
- Using two case studies as a basis, we will consider the nature of insider attacks and associated attacker profiles.
- We will also briefly consider insider threats within the cloud environment.
- Finally, we will review relevant mitigation strategies to address these threats.

Verizon Data Breach Investigations Report

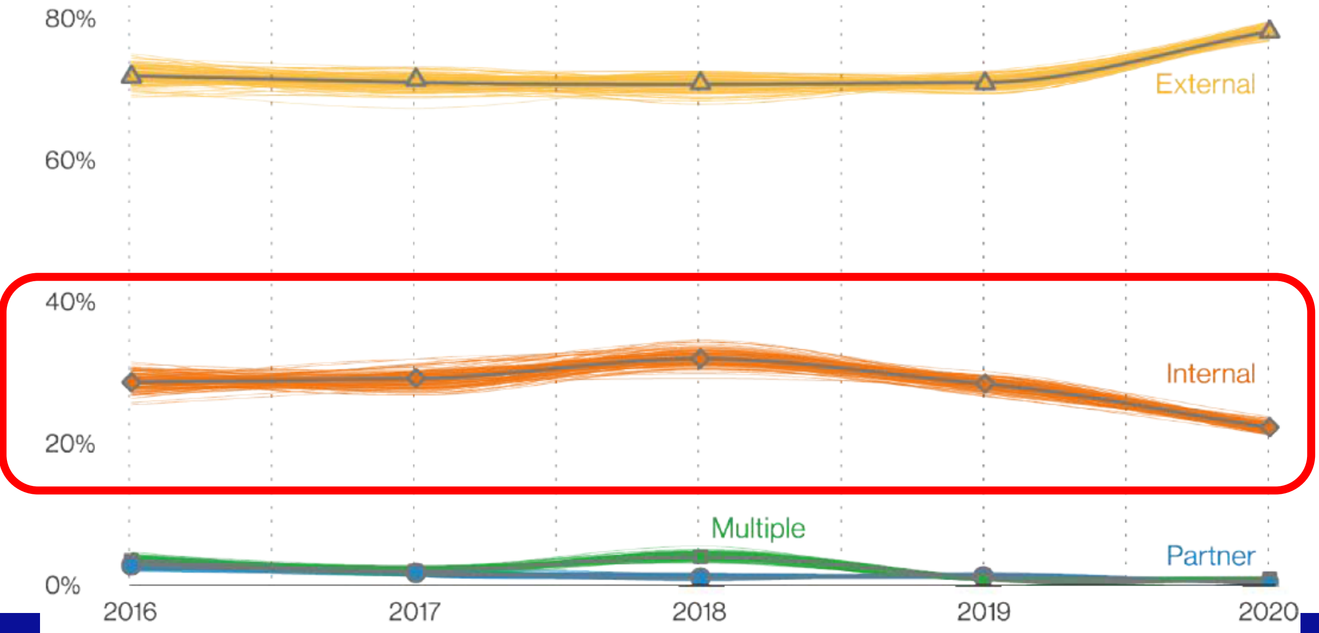


Figure 14. Threat actor over time in breaches

Source: Verizon's 2021 Data Breach Investigations Report, p.12, https://enterprise.verizon.com/resources/reports/2021-data-breach-investigations-report.pdf

Insider Attacks

Definition

- Inside Threat
  - *An entity with authorized access that has the potential to harm an information system through destruction, disclosure, modification of data, and/or denial of service.*[1]
- Insider Threat
  - *A malicious insider threat to an organization is a current or former employee, contractor, or other business partner who has or had authorized access to an organization's network, system, or data and intentionally exceeded or misused that access in a manner that negatively affected the* ***confidentiality****,* ***integrity****, or* ***availability*** *of the organization's information or information systems.*[2]

[1] SP 800-32 cited in Kissel, R., 2013. Glossary of Key Information Security Terms. NIST Interagency Reports, NISTIR 7298.

[2] US-CERT, 'Insider Threat', https://www.us-cert.gov/bsi/articles/best-practices/insider-threat

Insider Attacks – Drivers and Motivations

- **Drivers**
  - Malicious Intent
  - Complacency
  - Ignorance
- **Motivations**
  - Money
  - Revenge
  - Validation
  - Empowerment
  - Espionage

See Activity 1 – Insider Threats (under week 10)

Gelles, M 2016, 'Insider Threat : Prevention, Detection, Mitigation, and Deterrence', Elsevier Science, San Diego.

Detection stages and available tools

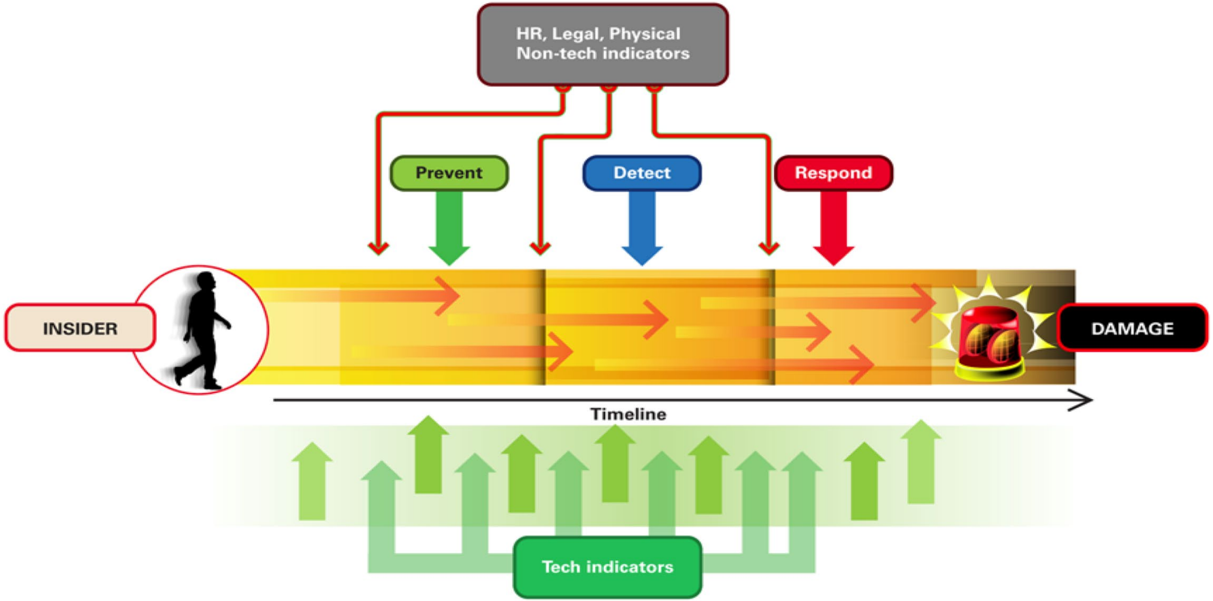


Figure 2. Opportunities for prevention, detection, and response for an insider attack

Source: Claycomb, W.R. and Nicoll, A., 2012, July. Insider threats to cloud computing: Directions for new research challenges. In Computer Software and Applications Conference (COMPSAC), 2012 IEEE 36th Annual (pp. 387-394). IEEE, p. 389.

Insider Attacks

- Insider attacks are usually planned, and it may therefore be possible to predict when an attack is going to occur, by identifying ‘red flags’ which are changes in attitude or behaviour.
- Examples include:
  - Growing frustrated or disgruntled.
  - Arriving early or staying late.
  - Showing interest in corporate information not related to their specific work.
  - Attempting to access restricted information.

Gelles, M 2016, ‘Insider Threat : Prevention, Detection, Mitigation, and Deterrence’, Elsevier Science, San Diego.

Additional Indicators of an Insider Threat

Digital Warning Signs

- Multiple requests for access to resources not associated with their job function
- Using unauthorized storage devices (e.g., USB drives)
- Network crawling and searches for sensitive data
- Data hoarding, copying files from sensitive folders
- Emailing sensitive data outside the organization

Behavioral Warning Signs

- Frequently in the office during off-hours
- Attempts to bypass security
- Displays disgruntled behaviour toward co-workers
- Violation of corporate policies
- Discussions of resigning or new opportunities
- Showing interest in corporate information not related to their specific work.

Insider Attacks

- Several frameworks have been proposed for detection, prediction and prevention of insider threats. We discuss an example of such an insider threat prediction model.

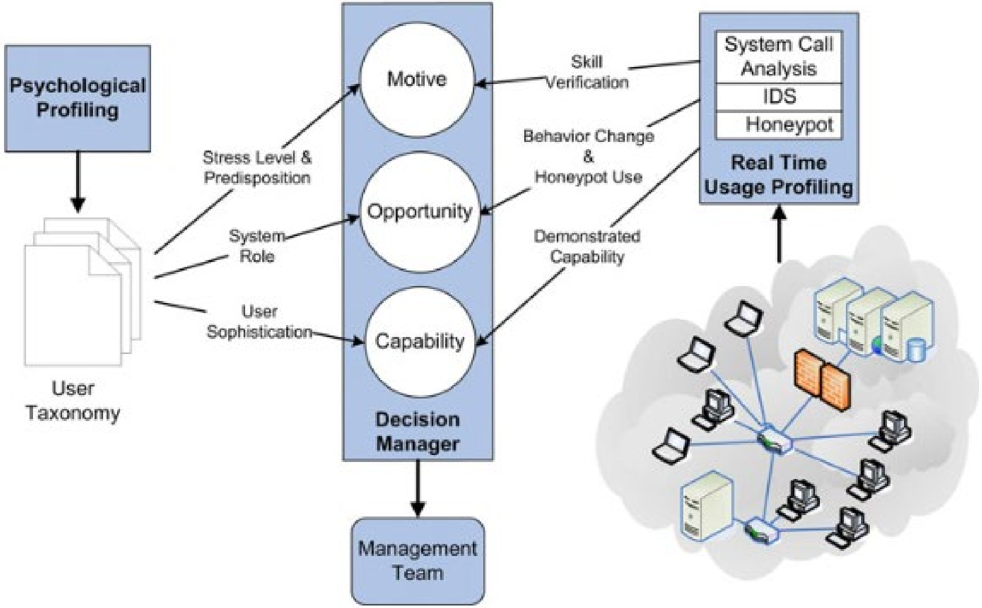
- This model utilises psychological profiling and technical indicators about users to predict the threat levels associated with different malicious insiders.

Alsowail, R 2021 ‘A multi-tiered framework for insider threat prevention’, MDPI-electronics, vol. 2021, no. 10, p. 9.
https://www.mdpi.com/2079-9292/10/9/1005

Source: Kandias, M, Mylonas, A, Virvilis, N, Theoharidou, M and Gritzalis, D 2010 ‘An insider threat prediction model’, in proceedings of International Conference on Trust, Privacy and Security in Digital Business, Springer, Berlin, Heidelberg, p. 29.
https://link.springer.com/content/pdf/10.1007%2F978-3-642-15152-1_3.pdf

Insider Attacks

Insider Threat Prediction Model



Source: Kandias, M, Mylonas, A, Virvilis, N, Theoharidou, M and Gritzalis, D 2010 ‘An insider threat prediction model’, in proceedings of International Conference on Trust, Privacy and Security in Digital Business, Springer, Berlin, Heidelberg, p. 29.

Insider Attacks

- User taxonomy / characteristics:
  - Stress Level {Low, Medium, High}
    - psychometric test that measures the current degree of personal and professional stress
  - Predisposition {Low, Medium, High}
    - questionnaire that measures the tendency of a user to demonstrate malevolent behavior
  - System Role {Novice, Advanced, Administrator}
    - this dimension reflects the access level of a user.
  - User Sophistication {Low, Medium, High}
    - questionnaire + capabilities

Source: Kandias, M, Mylonas, A, Virvilis, N, Theoharidou, M and Gritzalis, D 2010 ‘An insider threat prediction model’, in proceedings of International Conference on Trust, Privacy and Security in Digital Business, Springer, Berlin, Heidelberg, p. 29.

Insider Attacks

- Real-time usage profiling
  - System Call Analysis
    - alarm triggered for anomalous behaviour
  - Intrusion Detection System
    - detects known and unknown attacks
    - anomaly and signature based
  - Honeypot
    - evaluates whether a user is trying to exploit an opportunity to attack

Source: Kandias, M, Mylonas, A, Virvilis, N, Theoharidou, M and Gritzalis, D 2010 ‘An insider threat prediction model’, in proceedings of International Conference on Trust, Privacy and Security in Digital Business, Springer, Berlin, Heidelberg, p. 29.

Insider Attacks

- Motive
  - assessed using predisposition, current stress level and skill verification
  - input from System Call Analysis and IDS
- Opportunity
  - assessed using system role, behavior change and honeypot use
  - Input from System Call Analysis, IDS and Honeypot
- Capability
  - assessed using user sophistication, demonstrated capability
  - input from System Call Analysis and IDS

Source: Kandias, M, Mylonas, A, Virvilis, N, Theoharidou, M and Gritzalis, D 2010 ‘An insider threat prediction model’, in proceedings of International Conference on Trust, Privacy and Security in Digital Business, Springer, Berlin, Heidelberg, p. 29.

Insider Attacks

Requirements / Limitations:

- IDS depends on data being unencrypted
- Logging:
  - resources – space and the ability to analyse locally in order to avoid network transfers
  - expertise to analyse logs
  - automated communications with decision manager
- Social engineering attacks not detected
- Psychological profiling:
  - user skills vary widely across organisations
- Compliance with privacy concerns and legal constraints

Source: Kandias, M, Mylonas, A, Virvilis, N, Theoharidou, M and Gritzalis, D 2010 'An insider threat prediction model', in proceedings of International Conference on Trust, Privacy and Security in Digital Business, Springer, Berlin, Heidelberg, p. 29.

Insider Attack Case Study 1

Trade Secret Theft

Investigation into theft of intellectual property from GE leads to two guilty pleas.

- Jean Patrice Delia pleaded guilty to conspiring to steal trade secrets from General Electric Company (GE).
- The investigation showed that Delia and his partner Sernas stole elements of a computer program and mathematical model that GE used to expertly calibrate the turbines used in power plants.
- Because of their expertise, power plant operators from all over the world hired GE's performance engineers to help their turbines achieve peak performance for the climate and conditions in which they were installed.

https://www.fbi.gov/news/stories/two-guilty-in-theft-of-trade-secrets-from-ge-072920

Insider Attack Case Study 1

Trade Secret Theft

- ❑ Delia worked as a GE performance engineer for eight years, took a sabbatical in 2008 to study and returned in 2011.

Delia was a long term trusted employee

- ❑ Delia began downloading thousands of files from the company's system, including ones that contained trade secrets

What type of Insider was Delia?
What was his motivation?

- ❑ They then uploaded the files to the cloud or sent them to private email addresses.

What Signals were available for investigation?

- ❑ Delia also convinced an employee within the IT department to grant him access to files that he had no legitimate reason to see.

What type of Insider was the employee?

https://www.fbi.gov/news/stories/two-guilty-in-theft-of-trade-secrets-from-ge-072920

Insider Attack Case Study 1

Trade Secret Theft

- ❑ Those files contained the proposals and cost models GE used to bid on new work and contracts

What made this data valuable enough to steal?

- ❑ In May 2012, GE learned they had an unknown competitor on a bid to service a major power plant in Saudi Arabia. It was a company registered to Delia.

Which are the additional signs of an Insider attack?

- ❑ The FBI still had to prove it was Delia and Sernas. The FBI arrested Sernas and found he was traveling on company business, carrying a company laptop that had the GE trade secret files on it

- ❑ None of this was detected by GE’s cyber security systems. It was only picked up once GE lost a few bids.

https://www.fbi.gov/news/stories/two-guilty-in-theft-of-trade-secrets-from-ge-072920

Insider Attack Case Study 2

Information Theft

- A programmer reported that an application was experiencing unexpected failures.
- An investigation showed that ‘Mr. Simpson’ logged into the application server minutes before and reset service account passwords.
- He utilised these service accounts to collect data for interview use and to schedule jobs designed to disrupt workflows.
- When questioned, he confessed to using his administrative access to attempt to disrupt operations and download confidential files.

Verizon 2017, ‘Data Breach Digest’, http://www.verizonenterprise.com/verizon-insights-lab/data-breach-digest/2017/

Insider Attack Case Study 2

Information Theft

- Further forensic analysis determined that Mr. Simpson had also created jobs that would delete mass amounts of data on certain key dates.
- Finally, it was discovered that Mr. Simpson had installed a keylogger into a device that was sending data to a remote server in Romania.
- Mr. Simpson's actions were motivated by his unhappiness with the pending restructure of his work team.

Verizon 2017, 'Data Breach Digest', http://www.verizonenterprise.com/verizon-insights-lab/data-breach-digest/2017/

Insider Attacks in Cloud Environments

- Cloud computing opens up new opportunities for insider threats.
- Three types of cloud related insider threats:
  - Rogue administrator employed by a cloud provider.
  - Exploit weaknesses introduced by use of the cloud.
  - Using the cloud to conduct nefarious activity.
    - exploit processing power of cloud services
    - launch DDoS attack using cloud resources
    - exfiltrate data to the cloud

Claycomb, W.R. and Nicoll, A., 2012, July. Insider threats to cloud computing: Directions for new research challenges. In Computer Software and Applications Conference (COMPSAC), 2012 IEEE 36th Annual (pp. 387-394). IEEE.

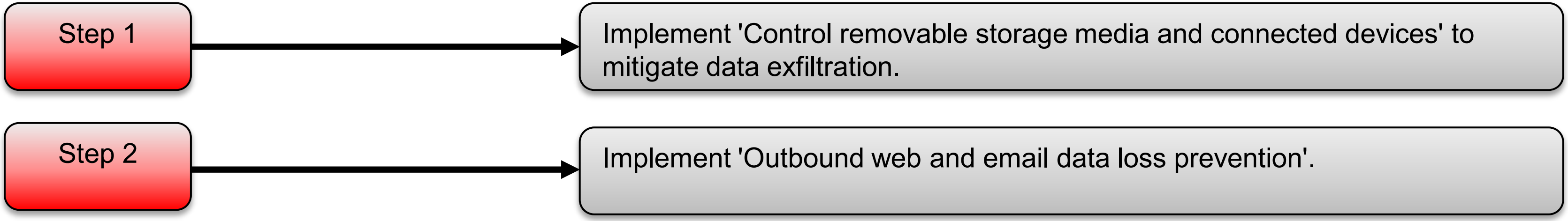
Insider Attacks in Cloud Environments

See Activity 2 – Cloud Insider Attacks (under week 10)

Insider Attack Mitigations

The ASD Strategies to Mitigate Cyber Security Incidents includes implementation strategies for both malicious insiders who steal data and those that destroy data.

The following is for insiders that steal.



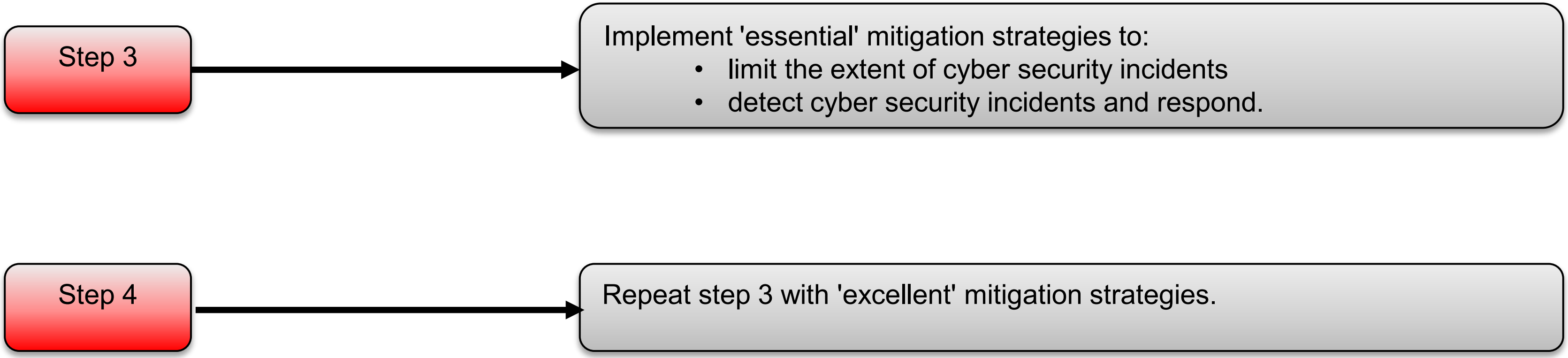
Step 1

Implement 'Control removable storage media and connected devices' to mitigate data exfiltration.

Step 2

Implement 'Outbound web and email data loss prevention'.

Insider Attack Mitigations



Step 3

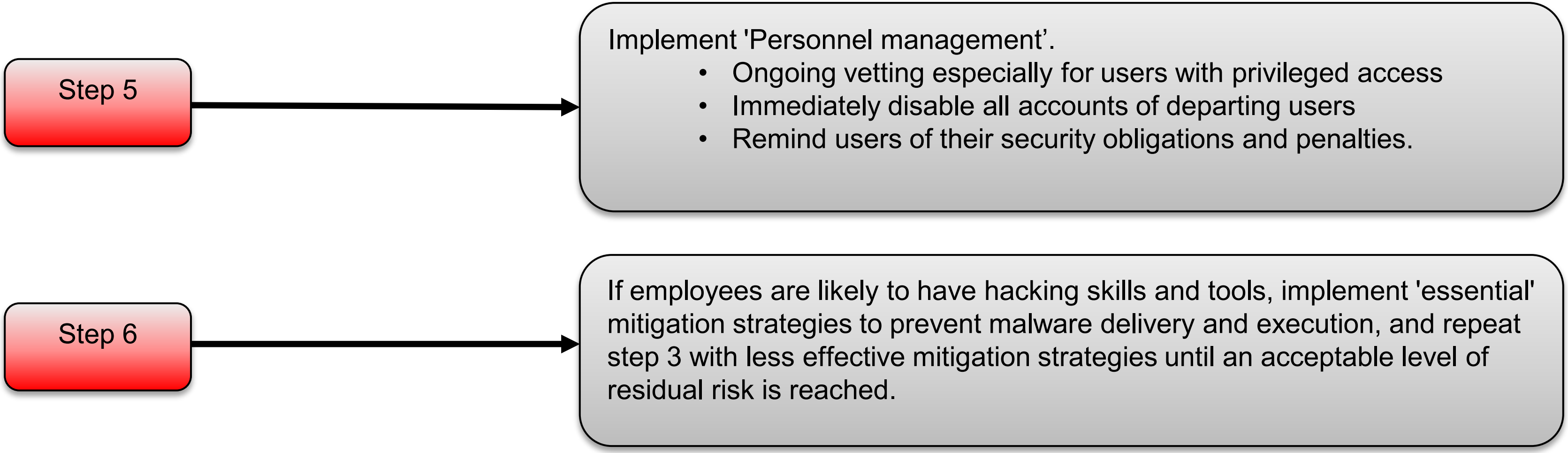
Implement 'essential' mitigation strategies to:

- limit the extent of cyber security incidents
- detect cyber security incidents and respond.

Step 4

Repeat step 3 with 'excellent' mitigation strategies.

Insider Attack Mitigations



Step 5

Implement 'Personnel management'.

- Ongoing vetting especially for users with privileged access
- Immediately disable all accounts of departing users
- Remind users of their security obligations and penalties.

Step 6

If employees are likely to have hacking skills and tools, implement 'essential' mitigation strategies to prevent malware delivery and execution, and repeat step 3 with less effective mitigation strategies until an acceptable level of residual risk is reached.

Insider Attack Mitigations

Technical controls

Control removable storage
Control outbound emails and files
Backups
Require strong passwords and multi-factor authentication

Access controls

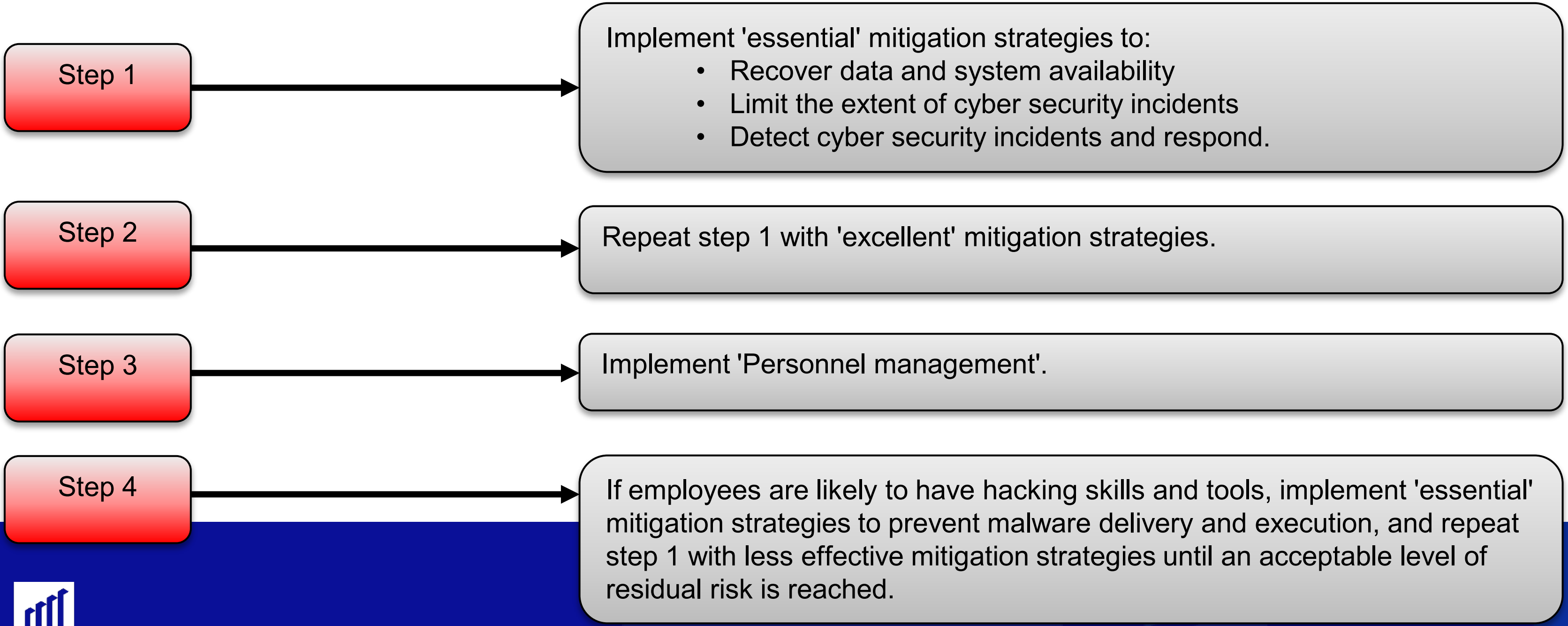
Restrict access
Use unique logons
Deactivate access

❑ Note that technical mitigation strategies provide incomplete security since data could be photographed or otherwise copied from computer screens or print-outs, or memorised and written down outside of the workplace.

Australian Signals Directorate2020, ‘Malicious Insiders’, https://www.cyber.gov.au/acsc/view-all-content/threats/malicious-insiders

Insider Attack Mitigations

Malicious insiders who destroy:



Step 1

Implement 'essential' mitigation strategies to:

- Recover data and system availability
- Limit the extent of cyber security incidents
- Detect cyber security incidents and respond.

Step 2

Repeat step 1 with 'excellent' mitigation strategies.

Step 3

Implement 'Personnel management'.

Step 4

If employees are likely to have hacking skills and tools, implement 'essential' mitigation strategies to prevent malware delivery and execution, and repeat step 1 with less effective mitigation strategies until an acceptable level of residual risk is reached.

Insider Attack Mitigations

Prevention & Mitigation

- Start a personnel security program
- Deter insider threat activities
- Ensure physical security
- Harden the digital environment (Part I & II)
- Prepare for organization changes

Detection & Validation

- Report suspicious insider activity
- Log and monitor user account activity
- Inventory and monitor sensitive data

Response & Investigation

- Activate the insider threat playbook
- Assemble the incident response team
- Collect and preserve evidence

Verizon’s 2017 Data Breach Digest Update, The Insider Threat: Protecting the Keys to the Kingdom, http://www.verizonenterprise.com/resources/reports/rp_data-breach-digest-2017-insider-threat_xg_en.pdf