

DPPC 20
24

**EMPOWERING YOU
THROUGH INFORMATION**

The basics of cyber incident response and actionable insights from recent investigations

Tuesday 8th October 2024

Aims and objectives



Develop a broad understanding of incident response and consider how the concept applies to your organisation.



Explore some of the key, actionable insights from recent ICO cyber investigations.



Consider the growing trend of ransomware “double extortion” and why data exfiltration matters.

Quiz time



Part 1 – Incident response

“The time to repair the roof is when the sun is shining”

Incident response

Source: Computer Security Incident Handling Guide (nist.gov)



Preparation

- Handling incidents
- Hardware and software
- Prevention



Detection & analysis

- Attack vectors
- Incident analysis and documentation
- Prioritisation
- Notification



Containment, eradication and recovery

- Containment strategy
- Evidence gathering
- Eradication and recovery



Post-incident activity

- Lessons learned
- Collecting evidence and retention

Quiz time



Part 2 – Actionable insights

“It is in the character of growth that we should learn from both pleasant and unpleasant experiences”

Actionable insight 1



Use MFA

- Mitigates common attack methods such as phishing and password spraying.
- Article 25 – Data Protection by design and by default.
- ICO guidance states it should be implemented wherever it is possible to do so.

Actionable insight 2



Vulnerability scanning

- Vulnerability scanning is an automated or semi-automated process that identifies security weaknesses.
- Penetration testing provides a deeper understanding of the security posture by actively testing defences and identifying weaknesses.

Actionable insight 3

Patch management



- Continuous monitoring and timely remediation of vulnerabilities.
- Critical or high-risk vulnerabilities (based on CVSS score) should be prioritised.
- How is patching approached by your organisation?

Actionable insight 4



Monitoring and alerting

- Controls in place to detect unusual or suspicious activity.
- This will likely vary significantly based on the size of the organisation and the data being processed.
- If resourcing is an issue, focus on critical assets.

Quiz time



Part 3 – The double extortion problem

“You can’t secure what you
can’t see.”

Actionable insight 5



Know what you have, know what it holds

- The systematic process of identifying, tracking and managing an organisation's assets.
- The ICO have an expectation an Information Asset Register will be in place.
- Consider obligations under Articles 33 and 34 of the UK GDPR.

Actionable insight 6



Logging and monitoring

- Recording events and activities that occur within a computer system or network.
- Structure logs in a way where the format is optimised.
- Secure logs via encryption at rest and in transit.
- Aggregate and centralise logs.

In conclusion...

- Develop an Incident Response plan and ensure its tested, properly implemented and receives buy in from key stakeholders.
- Enable MFA (where possible). If unavailable, embed other compensating controls.
- Have a process in place for vulnerability management.
- Monitor alerts and respond in a timely manner.
- Know what you have, know what it holds.
- Deploy logging best practices.



Q&A



#DPPC24

ico.org.uk/DPPC

