Cyber as a Service Risk: Protecting Public Services in a Digital Age

Safeguarding digital infrastructure against evolving cyber threats

Introduction and Context

Cyber as a Service Risk

Cyber Security is a Strategic Challenge

Cyber security affects frontline public service delivery and requires strategic organisational focus beyond IT.

Increased Exposure of Public Services

Digitally enabled public services like housing and social care face growing cyber threats, as we transform and enable digital channels we increase our attack surface.

Cyber Incidents as Service Continuity Risks

Cyber incidents are events that threaten the ongoing operation of essential public services, they need to be planned for in that context.

Role of Leadership in Cyber Risk

Leadership must understand and manage cyber risk alongside financial and operational risks to ensure resilience.

Understanding the Threat Landscape

Setting the Context

Evolving Cyber Threats

Public sector organisations face increasing frequency and sophistication of cyber attacks targeting data and services.

Critical Targets and Risks

The public sector manage sensitive data and infrastructure, making us all high-value targets for phishing, ransomware, and supply chain attacks.

Attackers

Due to the nature of our data and our profile we are targets for serious threat actors and state sponsored attacks.

Evidence of impact

There is no shortage of examples that can be used when discussing cyber attacks on the public sector. From Councils, to health boards to School trusts the fallout form incidents are well publicised.

Impact on Public Services

What a Cyber Incident Looks Like

Operational Disruptions

Cyber incidents disrupt critical systems, causing delays in business processes from housing repairs to financial transactions.

Impact on Vulnerable Service users

Social care outages limit access to vital information, risking support for vulnerable individuals.

Reputational and Trust Risks

Cyber incidents damage public trust, they can lead to investigations and fines and can divert the focus away from organisational priorities.

All consuming

An incident will occupy everyone from IT to Legal, Comms to Leadership, HR to Finance. This is not an incident to plan while its happening.

Recovery

Organisations who have experienced attacks report recovery in weeks, months and years rather than days.

Managing Cyber Risk

Managing risk

Inevitability of Cyber Incidents

Cyber incidents are unavoidable, think preparedness alongside avoidance.

Preparedness and Response

Organisations must focus on effective response plans and regular testing to manage and mitigate incidents.

Continuous Improvement and Resilience

Learning from past incidents and embedding cyber awareness across all levels enhances organisational resilience.

Understanding

An incident stops the delivery of functions, know your functions and the data and systems they depend on to prepare effectively.

Leadership and Responsibility

Why This Matters for Service Leaders

Leadership Ownership of Cybersecurity

Service leaders must actively engage in cyber risk management beyond technical teams to protect organisational services.

Risk Identification and Mitigation

Identifying critical systems and potential failure points helps service leaders plan for operational resilience during cyber disruptions.

Fostering a Security Culture

Leadership fosters a culture of awareness and accountability where staff understand their role in cyber incident prevention.

Integrating Cyber Risk in Governance

Embedding cyber risk into governance frameworks ensures clear reporting, senior oversight, and alignment with strategic risks.

Building Cyber Resilience

What Good Looks Like

Governance and Accountability

Leadership recognises cyber risks with clear accountability and strategic oversight to guide resilience efforts.

Protection and Secure Behaviours

Implement controls and promote secure staff behaviours to reduce attack likelihood and strengthen defenses.

Understand systems and data

Identify and minimize the attack surface, encrypt and backup critical data.

Detection and Monitoring

Monitor systems continuously to identify suspicious activities early and enable quick incident response.

Response, Recovery and Improvement

Use tested plans to manage incidents effectively, restore services quickly, and enhance resilience over time.

Collaboration and National Context

The Welsh Approach

Cyber Assessment Framework

CAF offers a structured method for assessing and enhancing cyber preparedness in public organisations with expert and peer support.

Collaborative Security Operations

A shared security operations centre has enabled resource pooling and intelligence sharing across Welsh public bodies.

Security community

A thriving community of security professionals share best practice, what works and what doesn't.

Aligned National and Local Efforts

Aligning local initiatives with national strategies enhances overall public sector cyber resilience.

Support and Key Takeaways

Key Actions

Cyber Risk Accountability
Treat cyber as a service risk with clear ownership and accountability at every organisational level.

Visibility
Make sure your departments know their processes and the associated systems and data that underpin them.

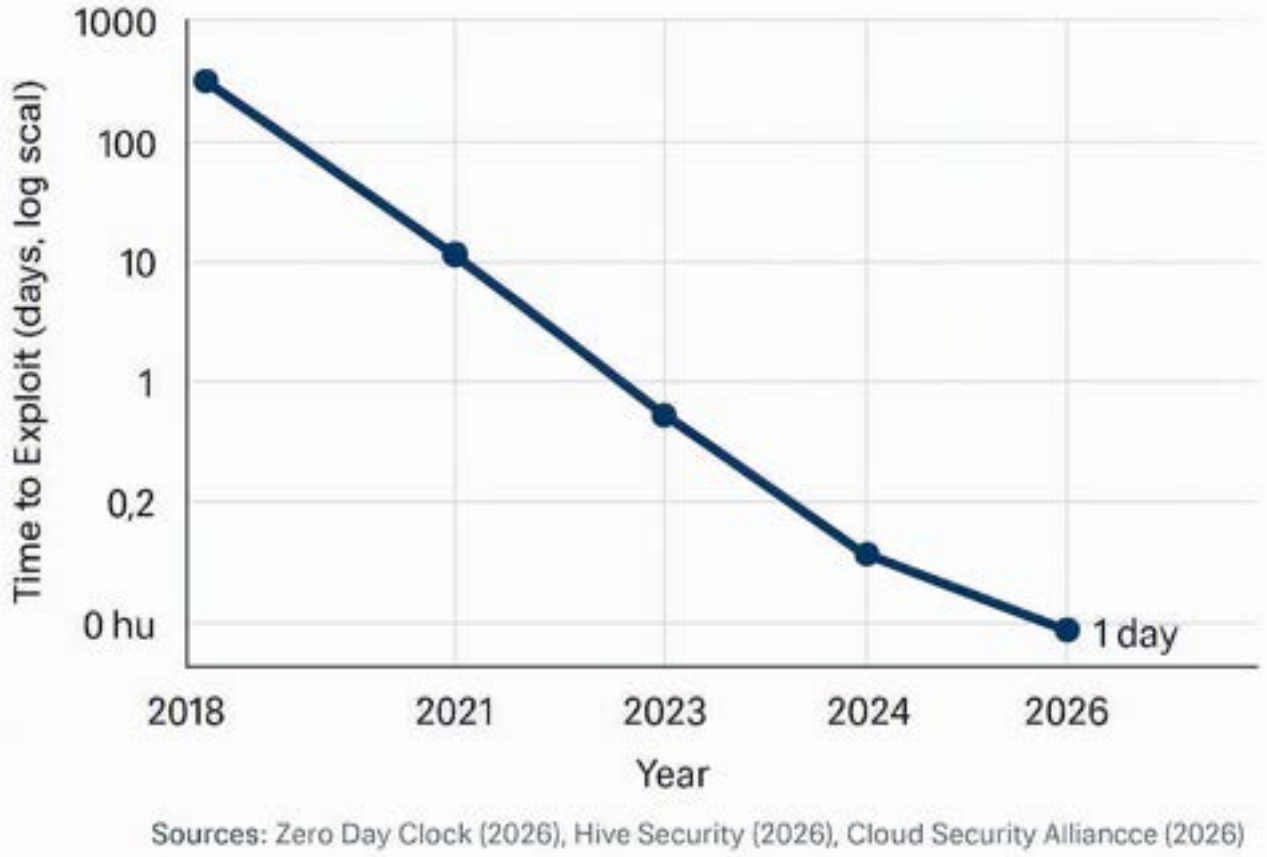
Response and Recovery Plans
Maintain tested response and recovery plans to ensure service continuity during cyber incidents.

Staff Awareness and Collaboration
Invest in staff training and collaborate with partners to strengthen cyber resilience.

Updates / patching
Work with your IT teams to ensure systems are up to date, this may mean some impact to the availability of services but is crucial.

Leveraging Sector Resources
Use sector-wide resources like Cyber@SOCITM and the Digital Trends report for guidance.

Emerging and developing threats
Keep one eye on the developments in the sector, be aware of AI's use to accelerate vulnerability detection and attack planning. The time you have to address a problem is rapidly decreasing.



TTE – Time to Exploit

Can we patch in time?

Questions?