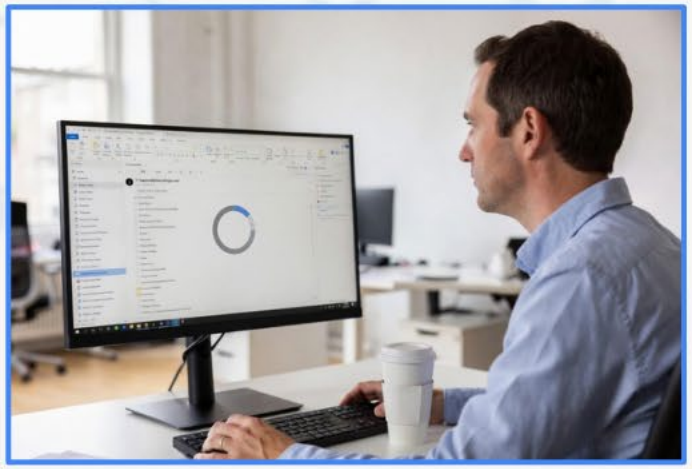
STRENGTHENING CYBER SECURITY ACROSS COUNCIL SERVICES

protecting our communities

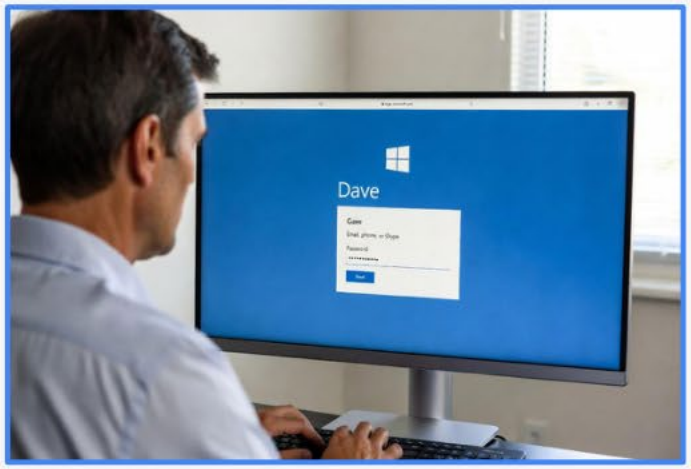
President's conference 2026

Cybersecurity Scenario

Dave opens Phishing email

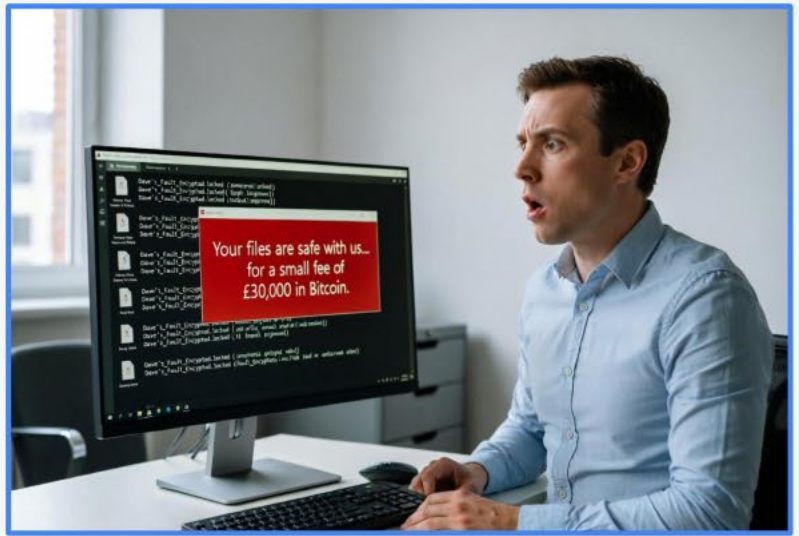


Enters password in fake Microsoft login



Hacked

Ransomware hits



Office chaos

Protection

"Remember, if you fail to prepare you are preparing to fail"
Rev. H.K. Williams, The Biblical World, 1919

People

- **The First Line of Defence - People as greatest strength and risk -** Universal, and targeted, education and training
- **Organisational commitment** - Ownership of cyber security from the top, funding
- **Culture -** Colleagues are confident openly discussing cyber risks

Processes

- **Proactive, not reactive, risk management** - Identify, assess, mitigate
- **Embed Cyber in ALL process** - at ALL stages of the digital lifecycle -- build or procurement, operate, decommission
- **Finger on the Pulse** - Threat informed planning and external awareness

Technology

- **Vendor management** - requirements, understand how vendors support org, assurance
- **Identity and access control -** increased relevance, distributed and partner working
- **The Right Products** - SIEM, Microsoft security suite, encryption products

Utilise existing resources and communities

CAF 4.0

NCSC Early warning service

Cyber@Socitim

Detection

'Prevention is better than cure.'
Desiderius Erasmus, 16th Century Philosopher

- **Defining Detection** - Identify malicious behavior, suspicious activity, or vulnerabilities across the entire council network.
- **Why Detection is Critical Now** - The Threat Landscape, Public Sector Vulnerability, The Human Element
- **The High Cost of Late Detection** - Average Cost, Industry Example, Service Impact
- **Strategic Opportunities for Improvement** - Improving Foundational Hygiene, Modern Security Models, National Frameworks, tools and training

Response

Goal: Minimise harm, maintain essential services, restore safely, and learn from incidents.

Key message: Cyber response is a whole-council resilience capability — not just an IT task.

Response lifecycle

0. Preparedness
Ongoing

- Have an emergency plan in place
- Practise it like a fire drill.

1. Assess & declare
0–30 mins

- Appoint lead
- Isolate systems

2. Contain & coord.
2–6 hrs

- Leaders/legal/tech
- Limit further spread
- Engage NCSC, ICO, NCA

3. Maintain services
Same day

- Manual workarounds
- Prioritise residents

4. Recover safely
Days after

- Restore backups
- Reset identities
- Support well being

5. Learn & improve
Post-inc.

- Review root cause
- Update plans
- Reflect & move on

Key response priorities

Clear leadership
Fast decisions on severity, escalation and ownership.

Strong communication
Keep staff, residents and partners informed.

Safe restoration
Restore critical services first and reconnect systems carefully.

NCSC: National Cyber Security Centre; **ICO**: Information Commissioner's Office; **NCA**: National Crime Agency;

Summary

1. Speed of Attack

- Cyber incidents escalate in minutes

2. Beyond Prevention

- Protect, detect and respond

3. People and process

- Clear roles. Confident teams

4. Shared Responsibility

- One council. One response

We cannot do this alone

But together — we are stronger

Council Considerations

Handling Highly Sensitive Data

Broad & statutory data remit:

- Councils carry extensive sensitive personal data that demands rigorous protection

Transparency & Accountability

Open by law:

- Councils operate under FOI laws and open data requirements that compel disclosure
- Security breaches easily become public knowledge, damaging trust

Diverse Workforce

- Complex human factor: reliance on contractors & shared services makes monitoring hard
- Human error and training gaps remain major issues

Resource Constraints

- Stretched budgets prioritise statutory services over cybersecurity
- Low per-employee security spend and legacy system vulnerabilities

Political Environment

- High-profile targets: vulnerabilities to politically motivated threats
- Intense scrutiny from media, ICO, and central govt compared to private sector

Opportunities

We may be vulnerable to cyber threat but **our network and commonality could be our biggest strength.**

How can we leverage these to create a more robust, shared infrastructure that protect us all from those targeting us through cyber crime?

Standardised Technology

- Standardised technology for our most high risk services
- Shared security operations centre (SOC) to monitor better and recover faster

Vendor Relationships

- Buying power increases collectively
- Collective supplier and supply chain assurance
- Collaborative development to support and influence government cyber policy

Joint Response Plans

- Shared response plans
- emergency recovery hubs
- additional support for high risk services during an incident

Collective Expertise

- Pool collective expertise to stay ahead
- Shared learning resources
- Inter council peer reviews
- Cyber team roundtables and knowledge sharing

Individually vulnerable. Collectively resilient.

Thank you for listening

Any questions?