Phish & Chips

London Borough of Barnet
London Borough of Hackney
London Borough of Hounslow
Norfolk County Council
Oxfordshire County Council

Contents

Examine how councils can evolve their cyber security capabilities to meet modern threats and support safe, sustainable digital services

Focus Areas: Protection | Detection | Response

40 Years of Cyber Security - Socitm

1986

The Computer Fraud and Abuse Act

The United States passes the CFAA, becoming one of the first major laws targeting unauthorized computer access and cyber crime

1988

Morris Worm

The Morris Worm becomes one of the first major internet worms, disrupting approximately 10% of the early internet and leading to the creation of the Computer Emergency Response Team (CERT)

1995

SSL Introduced

Netscape introduces Secure Sockets Layer (SSL), enabling encrypted web browsing and e-commerce security.

2000-2007

WORMS

ILOVEYOU, Code Red, SQL Slammer, Conficker - disrupting internet traffic, banking systems, automated and bot driven issues worldwide

2010s

Stuxnet & Malware

Cyber weapons, data destruction and ransom demands
Heartbleed, WannaCry

2018

GDPR Enforcement

The European Union begins enforcing the General Data Protection Regulation (GDPR), reshaping global privacy and cyber security compliance.

2020s

SolarWinds Supply Chain Attack

SolarWinds software updates, infiltrating governments and major enterprises globally.

2021

Log4Shell

The Log4Shell vulnerability in Apache Log4j creates one of the most severe internet-wide software security emergencies.

2022-23

LastPass Breach & Social engineering on the rise

Attackers compromised development systems

2024

Local Gov, Education, Libraries and Critical NHS Supply chain

Synnovis, Qilin ransomware

2025

AI Deepfake Fraud

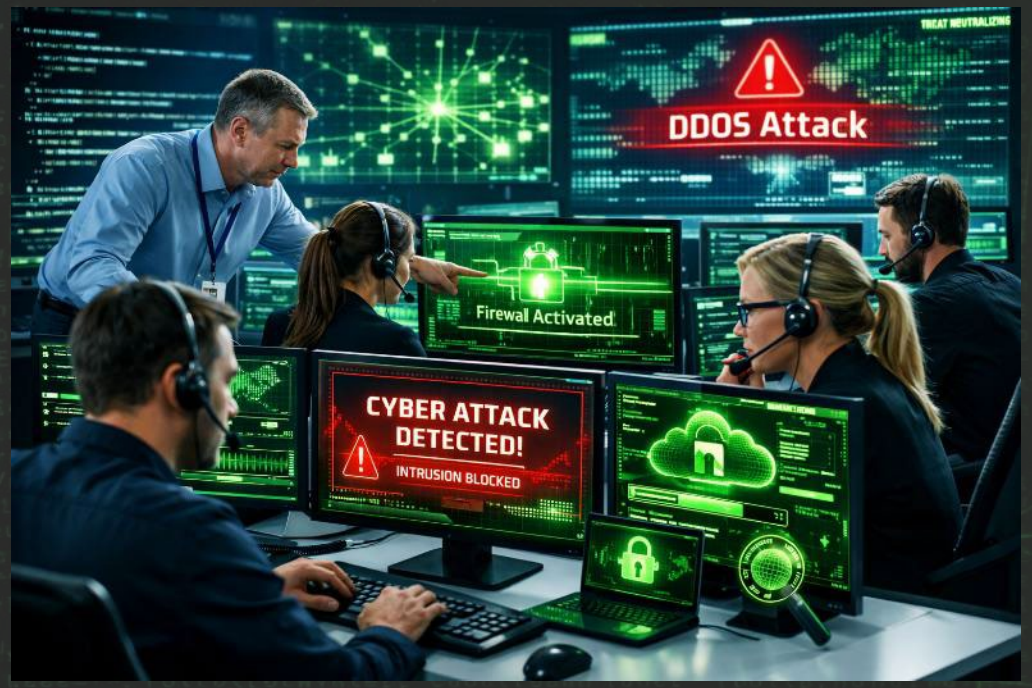
Manipulate evidence, undermine democratic institutions, trigger political change, erode trust in digital service

2026

Zero Trust and AI Driven Defense

Adopting zero trust, AI detection, automated response

The Modern Threat Landscape in Local Government



Cyber attacks are a **daily operational reality** for councils.

Key threats include ransomware, phishing, credential theft, and supply chain risks.

Hybrid IT environments (on-premise + cloud) increase complexity and exposure.

Disruption can lead to:

- Service Outages
- Financial Loss
- Loss of Public Trust
- Safety Events

Critical Insight:
Cyber security is no longer optional; it underpins public confidence and service resilience.

Focus Area: **Protection**

Strengthening Cyber Defences Across Local Government

Secure by Design
Defend as One

Definition: Preventing attacks by securing systems, users, and data.

Emphasis on consistent, organisation-wide controls:

- Multi-factor authentication, encryption, firewalls, antivirus, passkeys
- Regular patching and vulnerability management
- Network segmentation and offline, tested backups
- Staff awareness across all roles (not just IT)
- Change is essential but brings risk

Key Evolution:

- From perimeter-based security → Zero Trust / identity-focused security
- From IT responsibility → Whole-organisation responsibility
- Demand for skills

Strategic Opportunity:

Embed security into procurement, design, and digital transformation

Protection: The Human Element

Develop the right cyber security skills, training knowledge and culture

- Basic tools and skills to identify an issue.
- Confidence to report it.
- Training that builds knowledge and provides clarity and confidence in what steps to take both at work, and at home.
- The right training, with the right message could stop something before it does harm.

Focus Area: **Detection**

Enhancing Cyber Threat Visibility Across Local Government

Detection

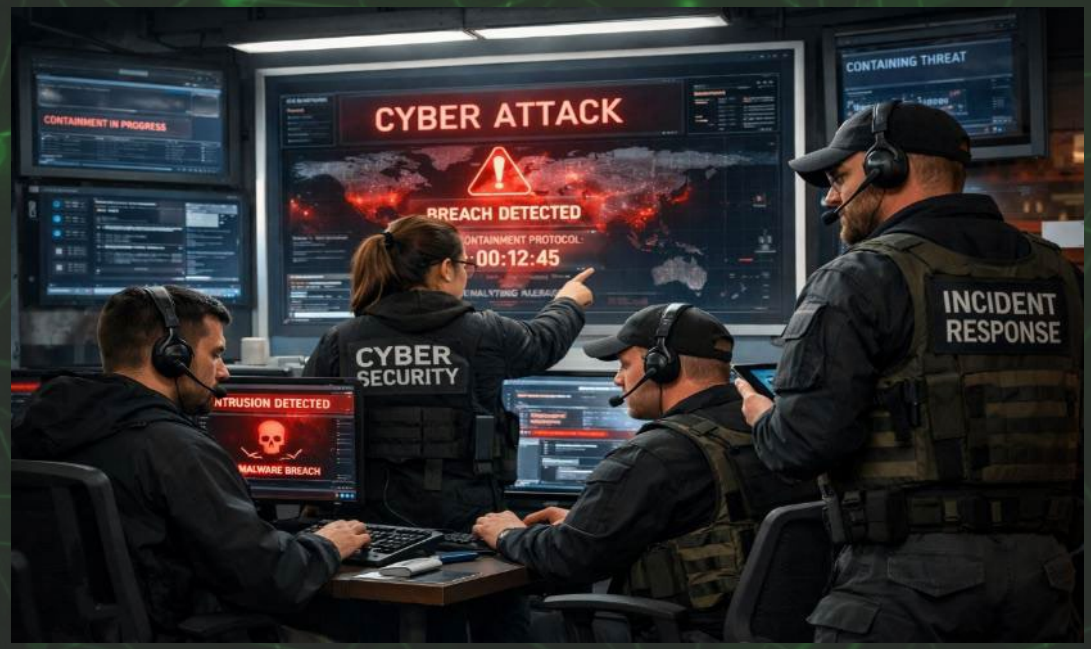
Detection is critical for identifying cyber threats early and reducing impact on council services.

Key objectives and capabilities include:

- Identify key detection risks
- Assess current monitoring and visibility capabilities
- Develop demonstration scenarios
- Provide actionable recommendations for improvement
- Explore scalable detection solutions (SIEM, XDR, SOC models)

Detection Challenges

- Limited visibility
- Managing detection
- Skills shortages
- High volume of alerts
- Budget and resource constraints
- Increasing sophistication



Detection - Tools and Approaches

Detection is the bridge between a potential breach and a full-blown crisis. Because councils handle a mix of sensitive citizen data (social care, tax records) and critical physical infrastructure (traffic lights, waste management), detection must be multi-layered.

The main aspects of cyber security detection tailored for local government are:

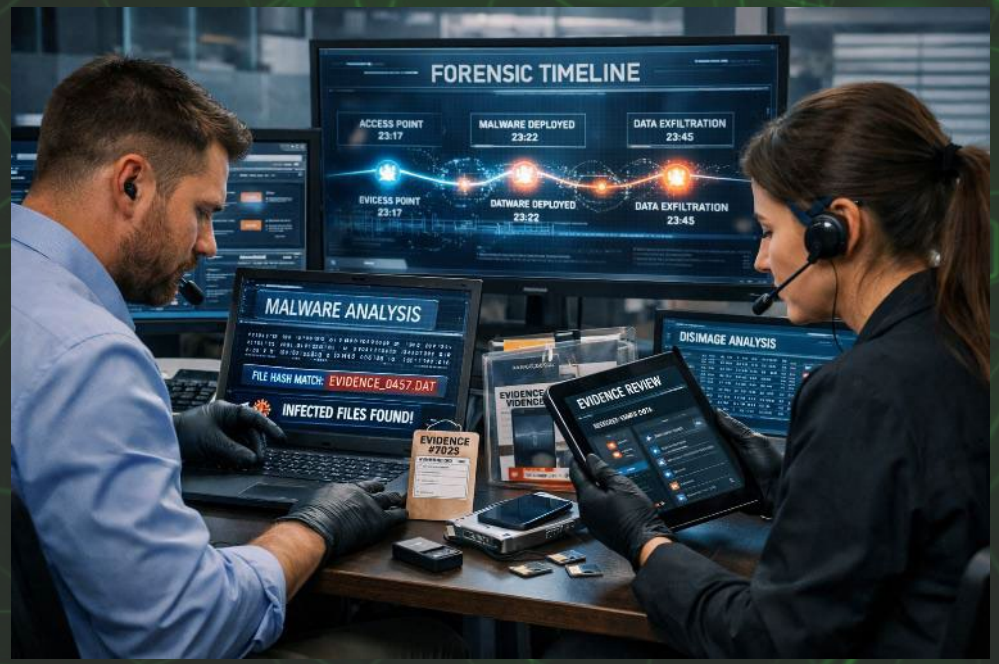
- Security Monitoring & Visibility
- Advanced Endpoint Detection
- Network & Perimeter Analysis
- Proactive & Human-Centric Detection
- Governance & Frameworks

Detection - The Human Element

There is a much-overlooked side to detection, and this relates to staff. Breaches are often facilitated through highly complex spam, and phishing campaigns. Even if staff are adequately trained in data awareness, and cyber security, these approaches can still be successful. However, if councils foster an open, and transparent culture, staff are more likely to come forward even if they believe they may have fallen prey to such a campaign.

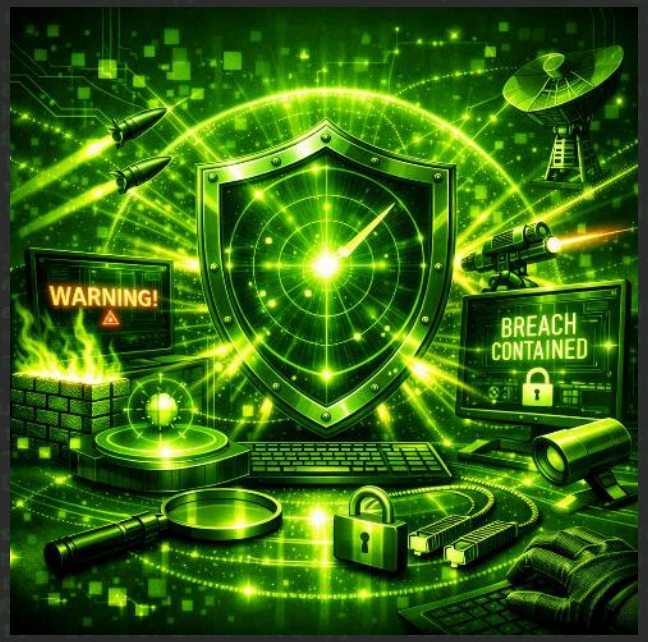
Detection - Recommendations

- Centralised monitoring and SOC capabilities
- Improved visibility across cloud, identity, and endpoints
- Enhanced Threat intelligence
- Strengthen vulnerability management processes
- Cyber skills and council partnerships
- Automation to reduce response times
- Awareness amongst users
- Mandatory awareness / cyber-security training
- Culture of transparency and openness

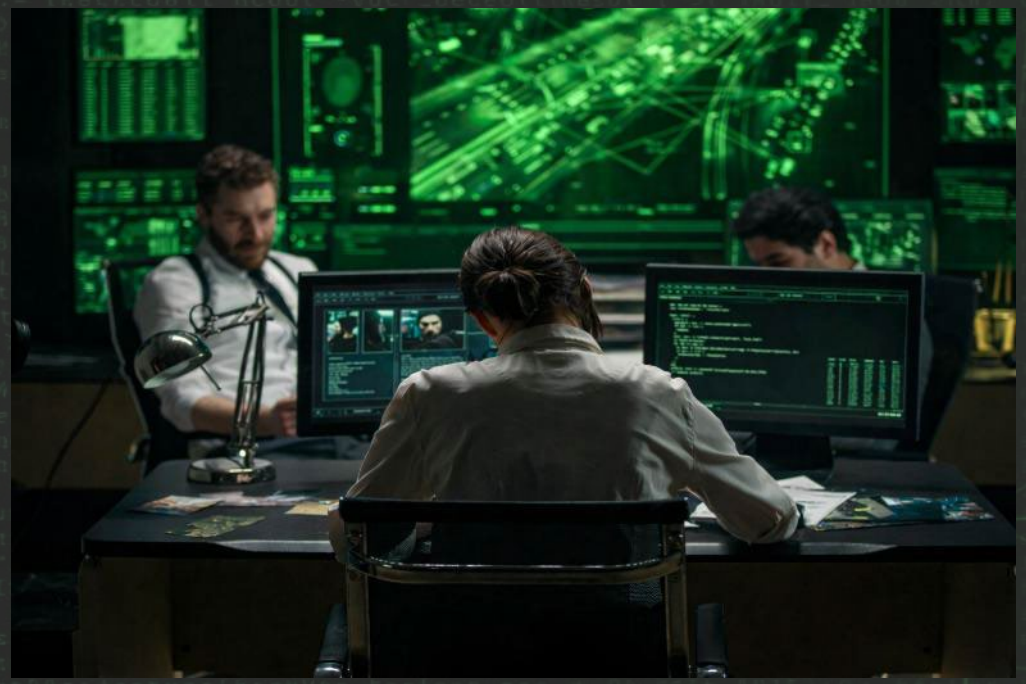


Focus Area: **Response**

Building Cyber Resilience in Local Government

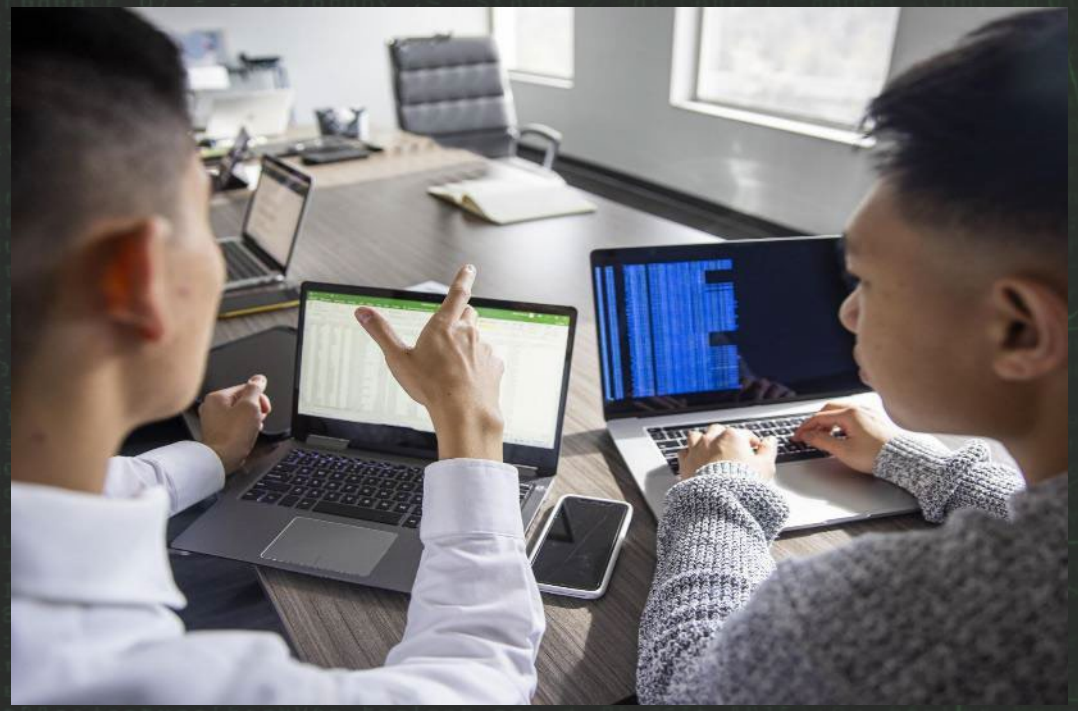


Incident Response Planning and Service Restoration



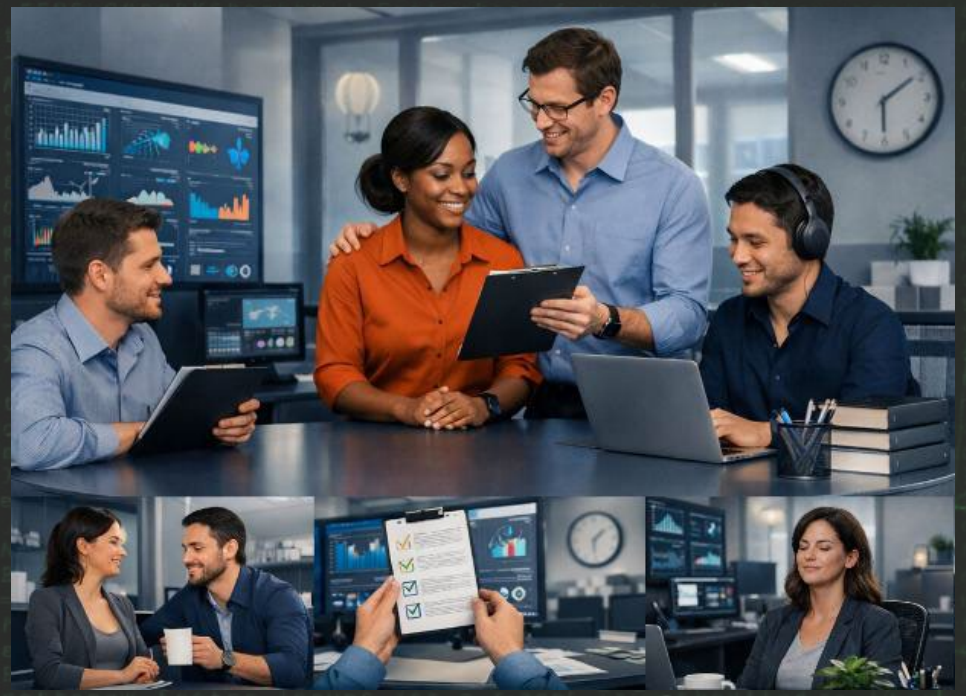
- Structured Incident Response
- Regular Plan Testing
- Business Continuity & Recovery
- Rapid Service Restoration

Preparation, Leadership, and Continuous Improvement



- Ongoing Preparation
- Leadership Engagement
- Continuous Improvement
- Data Integrity and Backup

Look After Your People



- Prioritise Communication
- Safeguard Mental Health & Wellbeing
- Provide clear support options

Building resilient, secure, and sustainable digital services requires the right people, processes, and technology to enable us to DEFEND AS ONE.

Thank You For Listening