Leicestershire County Council

Update on the Councils Cyber Security Approach

Jan ‘25

Agenda Item 10

Real World Examples

Copeland Borough Council

- Suffered malware attack during August Bank Holiday in 2017
- LA lost access to all data including use of majority of computers
- Council cut off from other partners to avoid cross-contamination
- Council had to revert to pen & paper
- Est. cost (as at Oct 2019) £2.5m

Redcar & Cleveland BC

- Suffered ransomware attack in Feb 2020
- 95% data encrypted
- 4 weeks to restore 2/3rd of systems
- Estimated recovery cost £10.4m (10% of budget)

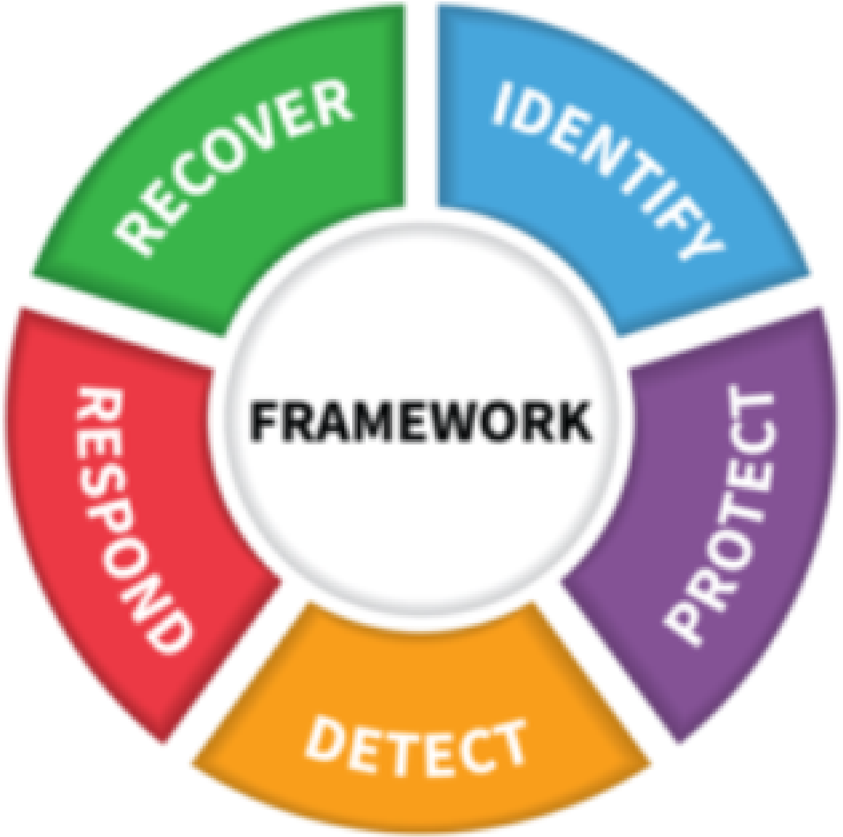
Leicester City Council

- Full impact unknown however significant effort required in updating staff equipment
- Implementation of 2-factor authentication software
- Replacement of Virtual private network infrastructure

Approach

Our approach is based on the NIST (National Institute of Standards and Technology) framework, which cover 5 areas:

- ✓ **Identify**
- ✓ **Protect**
- ✓ **Detect**
- ✓ **Respond**
- ✓ **Recover**

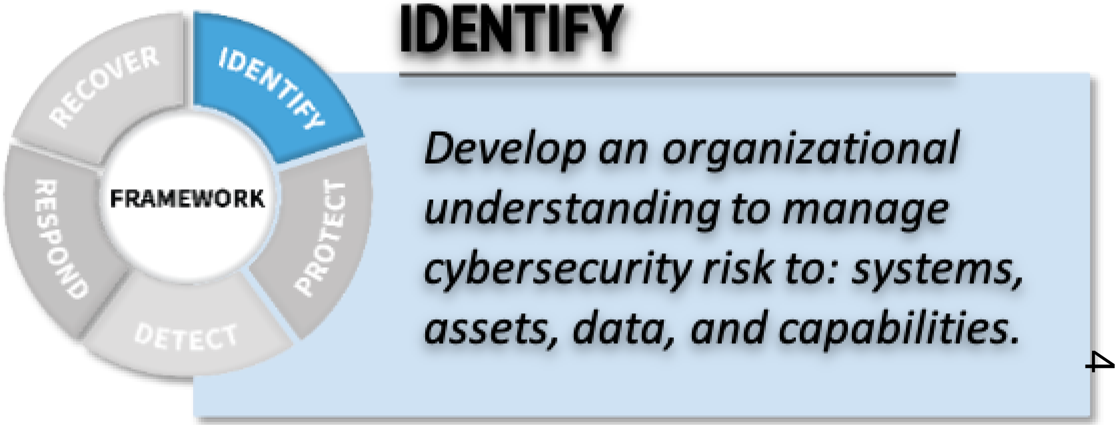


IDENTIFY

We do this through a comprehensive asset management process supported by strong governance, risk management and change management processes. Future requirements are mapped out on our Cyber Security roadmap.

Alongside this, we also continue to ensure we achieve our Public Services Network (PSN) accreditation every year. This Accreditation requires a third-party assessment of our security position and involves scanning our network and systems for known vulnerabilities that must be resolved before the accreditation can be awarded. The accreditation is awarded by the Cabinet Office.

Key IT controls are also subject to annual internal and external audits



IDENTIFY

Develop an organizational understanding to manage cybersecurity risk to: systems, assets, data, and capabilities.

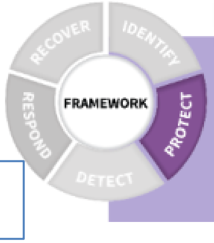
The number of vulnerabilities flagged by an external health-check can be immense and takes significant IT effort to remedy.

PSN ★★★ APPROVED

Cabinet Office

PROTECT

We use a “defence in depth” approach to stop attackers gaining access to our systems and data, this means using a combination of technologies and practices to make it as hard as possible to break in.



PROTECT

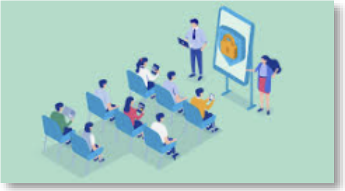
Develop and implement the appropriate safeguards to ensure delivery of services.

Client Defences

End Point Protection through advanced Anti Virus software

Strong password management for network, application and 3rd party access to our systems.

Training & awareness through Security & GDPR courses provide staff with simple do’s & don’t when it comes to security



Network Defences

Data Protection systems provide the ability to recover business critical systems and data in the event of a disaster or cyber event.

hyper-converged infrastructure which is home to LCC’s virtual environment with its own inbuild security & encryption capabilities.

Hardened Operating Systems on Servers and laptops through security controls and local firewalls which adds additional layers of protection for our critical data.

SIEM provid0es visibility of what is going on in the network

Perimeter Defences

Multi-layer firewalls provide perimeter in and inner network protection from external vulnerabilities

Secure Email Gateways provide an enhanced layer of protection for Microsoft Office 365 email services

Virtual Private Network (VPN) technology provides a secure mechanism for corporate laptops to connect back to the LCC network from the internet.

Above technical platforms are supported by key foundational operational processes

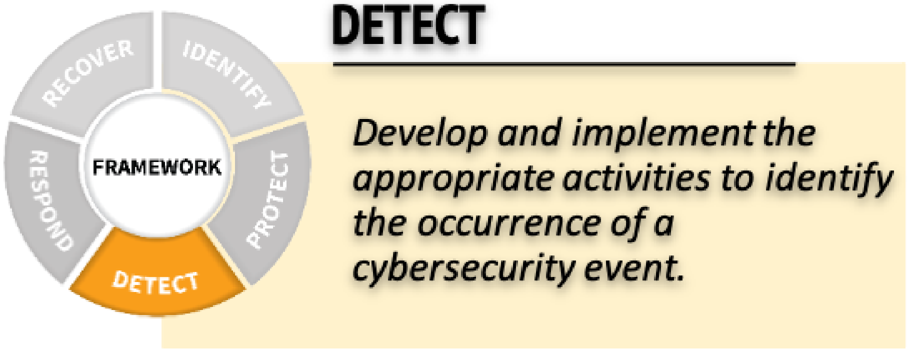
- System Patching
- External IT Health Checks
- Reacting to 3rd party Vulnerability Notification
- Review Platform Capability
- Vendor Engagement
- Good Governance & Policies
- Knowledge & Awareness across the organisation

DETECT

If hackers do gain access, we need to be able to “see” that our defences have been breached and act as quickly as possible to block the attack and minimise the damage done.

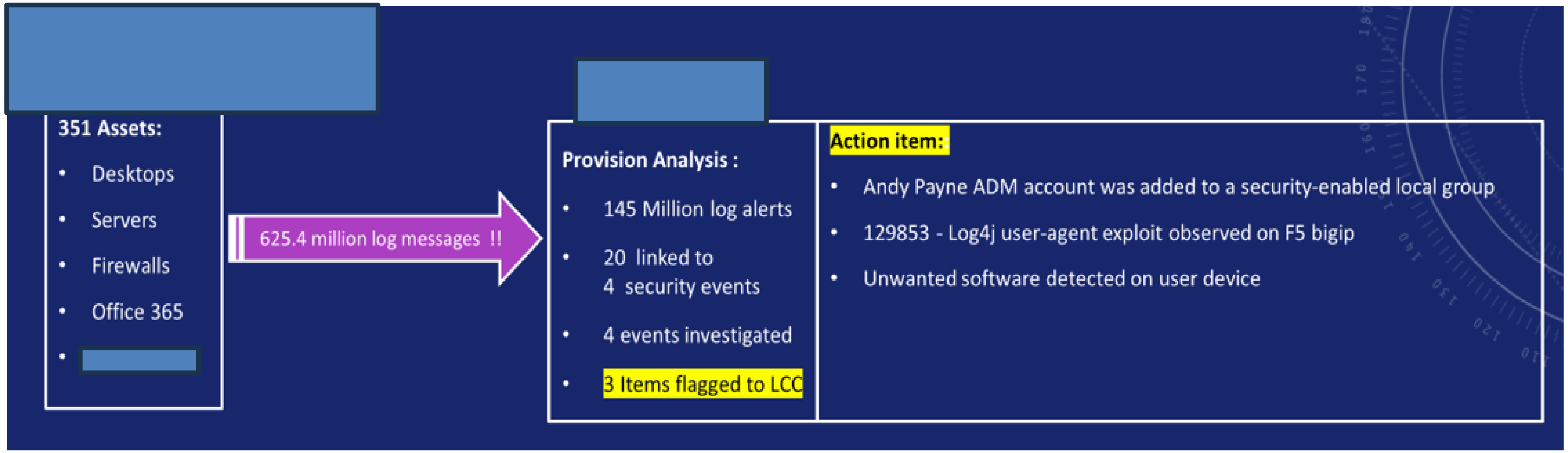
What we have in place to support this:

- Internal Monitoring Tools
- Security Information & Event Management (SIEM) Service



DETECT

Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.



[redacted]

351 Assets:

- Desktops
- Servers
- Firewalls
- Office 365
- [redacted]

625.4 million log messages !!

[redacted]

Provision Analysis :

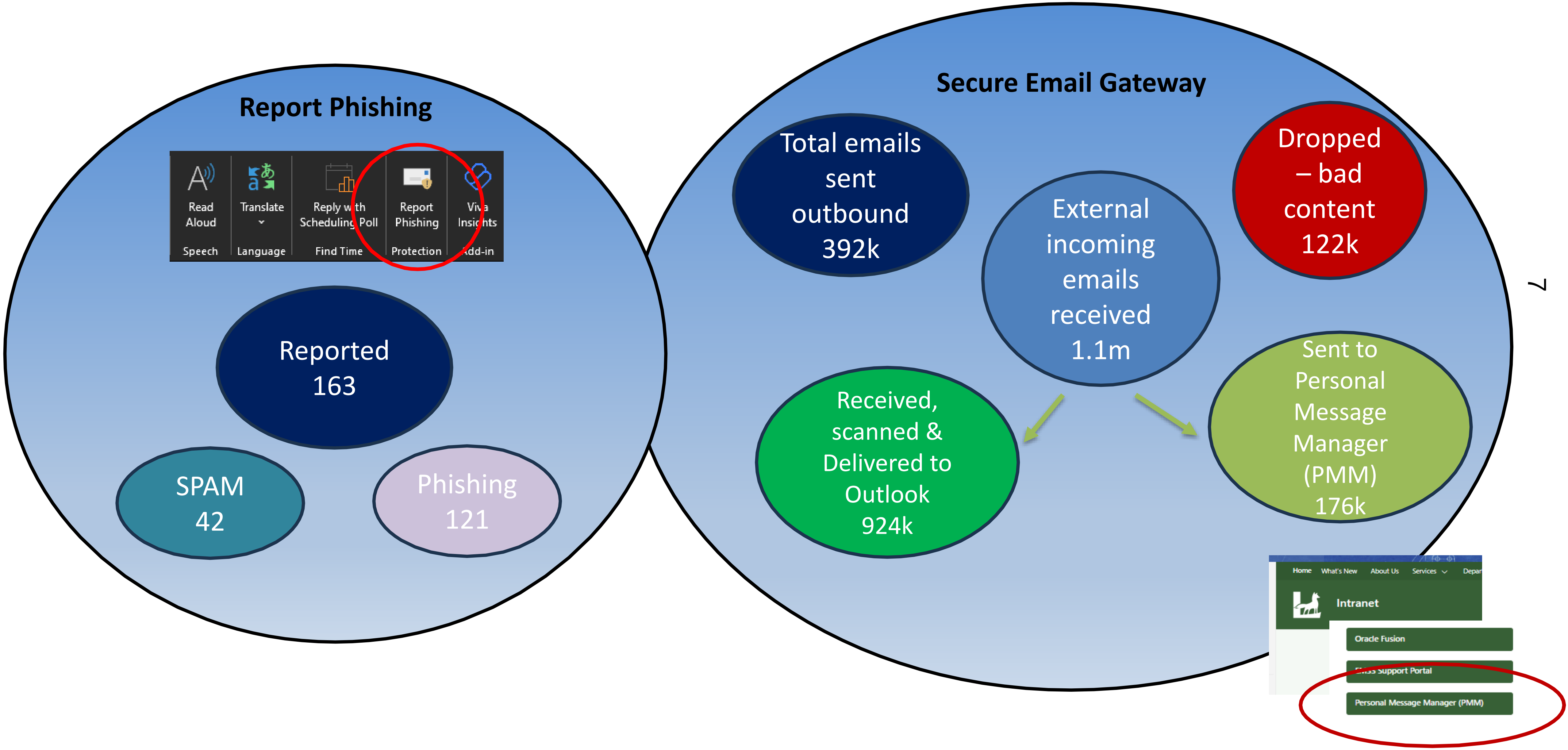
- 145 Million log alerts
- 20 linked to 4 security events
- 4 events investigated
- 3 Items flagged to LCC

Action item:

- Andy Payne ADM account was added to a security-enabled local group
- 129853 - Log4j user-agent exploit observed on F5 bigip
- Unwanted software detected on user device

DETECT - EMAIL

Leicestershire County Council



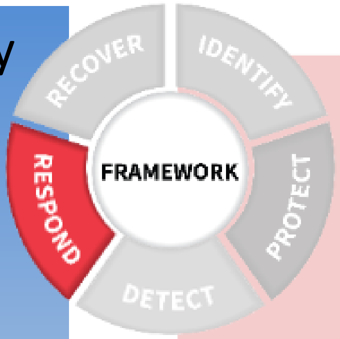
Report Phishing
Read Aloud
Translate
Reply with Scheduling Poll
Report Phishing
Viva Insights
Speech
Language
Find Time
Protection
Add-in
Reported 163
SPAM 42
Phishing 121
Secure Email Gateway
Total emails sent outbound 392k
External incoming emails received 1.1m
Dropped – bad content 122k
Received, scanned & Delivered to Outlook 924k
Sent to Personal Message Manager (PMM) 176k
Home
What's New
About Us
Services
Depar
Intranet
Oracle Fusion
ss Support Portal
Personal Message Manager (PMM)

RESPOND

Once an attack is identified we need to be able to deal with it quickly and professionally.

Our Cyber incident plan gives a structured approach on how to deal with Cyber threats, as well as detailing key contacts, both internally and externally.

These external contacts include the NCSC (National Cyber Security Centre), The Police Cyber Crimes Department and our Cyber Incident Response partner.



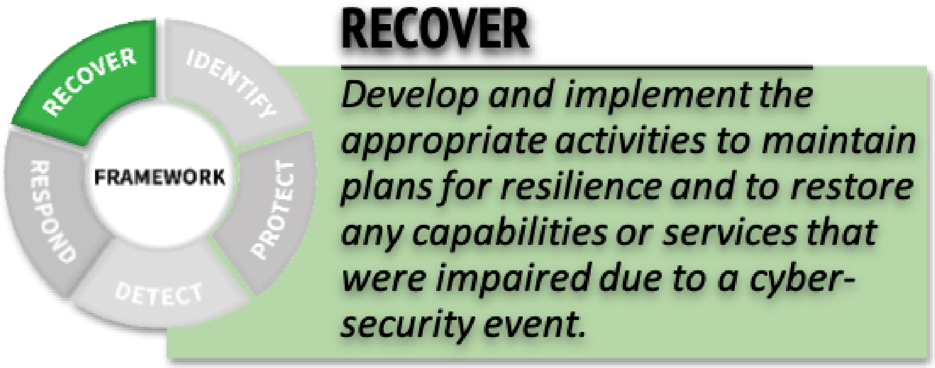
RESPOND

Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.

Some vulnerabilities require **immediate attention** – recent vulnerability identified by a supplier that affected LCC systems reacted to urgently, affected systems were patched within 24hrs of receiving notification. This demonstrated a reactive IT team with robust processes.

RECOVER

No security is 100% infallible and so we need to ensure we are ready to bring systems back online should an attack prove successful.



RECOVER

Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cyber-security event.

Systems and Recovery mechanism key to system and service recovery include:

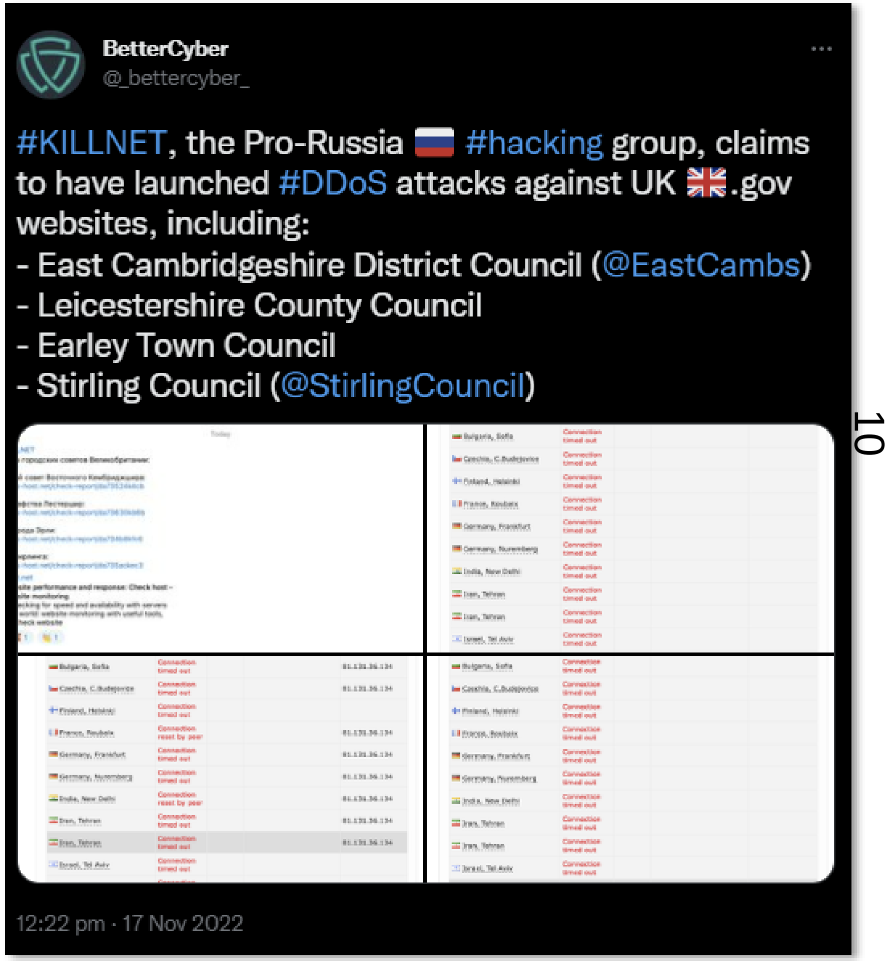
Robust Business Continuity (BC) Plans – a series of desktop activities have been undertaken between the BC Team and Departmental leads in recent months to improve departmental preparedness in a BC situation

- **Comprehensive Disaster Recovery (DR) Process & Practise** – DR Steering Group convene regularly to govern DR activities and testing, reporting to Resiliency Planning Group
- **Technology** – Significant investment made in **Data Protection and systems ,**which will play a critical part in recovery if/when we suffer an attack, and data & systems are impacted
- **3rd Party Support** – Help from the likes of NCSC, Police etc will be essential to assist in the technical recovery, as well as internal Comms Teams for media handling.

TYPES OF THREATS WE FACE

Leicestershire County Council

- Ransomware
- Nation state interference – democracy & elections
- Third party suppliers
- Phishing
- Artificial Intelligence
  - Distributed Denial of Service (DDOS) attacks



BetterCyber
@_bettercyber_

#KILLNET, the Pro-Russia 🇷🇺 #hacking group, claims to have launched #DDoS attacks against UK 🇬🇧.gov websites, including:
- East Cambridgeshire District Council (@EastCambs)
- Leicestershire County Council
- Earley Town Council
- Stirling Council (@StirlingCouncil)

Today

NET
городских советов Великобритании:
совет Восточного Кембриджшира
host.net/check-report/[illegible]
рфетон Лестершир:
host.net/check-report/[illegible]
ода Ерли:
host.net/check-report/[illegible]
ерлинга:
host.net/check-report/[illegible]
net
site performance and response: Check host - site monitoring
cking for speed and availability with servers world: website monitoring with useful tools. Check website

Bulgaria, Sofia	Connection timed out
Czechia, C.Budejovice	Connection timed out
Finland, Helsinki	Connection timed out
France, Roubaix	Connection timed out
Germany, Frankfurt	Connection timed out
Germany, Nuremberg	Connection timed out
India, New Delhi	Connection timed out
Iran, Tehran	Connection timed out
Iran, Tehran	Connection timed out
Israel, Tel Aviv	Connection timed out

Bulgaria, Sofia	Connection timed out	81.131.36.134
Czechia, C.Budejovice	Connection timed out	81.131.36.134
Finland, Helsinki	Connection timed out	
France, Roubaix	Connection reset by peer	81.131.36.134
Germany, Frankfurt	Connection timed out	81.131.36.134
Germany, Nuremberg	Connection timed out	81.131.36.134
India, New Delhi	Connection reset by peer	81.131.36.134
Iran, Tehran	Connection timed out	81.131.36.134
Iran, Tehran	Connection timed out	81.131.36.134
Israel, Tel Aviv	Connection timed out	

Bulgaria, Sofia	Connection timed out
Czechia, C.Budejovice	Connection timed out
Finland, Helsinki	Connection timed out
France, Roubaix	Connection timed out
Germany, Frankfurt	Connection timed out
Germany, Nuremberg	Connection timed out
India, New Delhi	Connection timed out
Iran, Tehran	Connection timed out
Iran, Tehran	Connection timed out
Israel, Tel Aviv	Connection timed out

12:22 pm · 17 Nov 2022

LAST 12 MONTHS

Leicestershire County Council

Policy, Process & Governance

- PSN Compliance – Achieved until April ‘25
- Refreshed Information Security e-Learning package
- External Cyber Security Audit/Assessment & Social Engineering Exercise
- Renewal of contract for Cyber Incident Response Retainer Service
- Cyber Resilience
  - Testing of departmental BC plans
  - Disaster Recovery testing (DR Steering Group)

Technology Improvements

- Replacement “Data Backup” solution
- Rollout of new anti-virus tool and policies to laptops and servers
- Security Information and Event Management (SIEM) Platform
- Added “Report Phishing” tool in Outlook
- Forced reboots on laptops to support security patching process
- Compliance monitoring of corporate Smartphone security updates

NEXT 12 MONTHS - HIGHLIGHTS

- Office and member awareness
- 12-month Comms campaign
- Procurement templates – review & update standard security requirements
- Continue to ensure we achieve our PSN accreditation
- Cyber Resilience
    - Continuation of Disaster Recovery testing
    - Departmental BC plan reviews

PERSONAL CYBER SECURITY

What's good practice at work also applies at home:

- Strong passwords, three random words approach
- Use 2-factor authentication where possible
- Keep your software and devices up to date
- Ensure you have anti-virus software installed and it’s up to date

- Be vigilant with potential Phishing E-mails and never click on links in E-mails that you are not 100% sure about
- If you’re not sure, click the “report phishing” button in Outlook or contact the IT Service Desk

THANK YOU FOR LISTENING

Questions ?