Briefing: Understanding PCC's Cyber Risks and How the Organisation is Responding

Scrutiny Management Board

Introduction

The digital transformation of Plymouth City Council has created service improvements for residents and efficiencies for the Council, whilst also establishing new and greater dependencies on our IT. We have never relied more on our IT to deliver essential public services, manage sensitive citizen data, and support local democracy. At the same time the sophistication and proliferation of cyber-attacks has risen with public services being targeted by well-resourced criminals and state backed groups. These cyber attacks threaten the systems and data we now rely upon for services and leverage the impact on residents as well as the reputational damage and cost to the Council as a threat against us. This briefing provides an overview of the current cyber threat landscape facing all UK local authorities, examines the most common attack types, and describes the actions we are taking to continue to strengthen our cyber resilience.

The Cyber Threat Landscape

Local authorities are attractive targets for cyber criminals due to the volume and sensitivity of the data they hold, the essential nature of their services, and, in some cases, the limited resources available for cyber defence. Attackers range from opportunistic criminals to sophisticated nation-state actors, hacktivists, and insider threats. The consequences of a successful cyber attack can be severe, including service disruption, financial loss, data breaches, reputational damage, and legal liabilities.

Key Trends Affecting Local Authorities

Increased digitisation of public services and remote working has expanded what is called our attack surface. Attack surface simply means the number of devices that are exposed to internet and therefore potentially vulnerable to attack.

Integration with third-party vendors and cloud services introduce potential supply chain vulnerabilities.

Ransomware attacks are rising, often targeting public sector bodies with critical service responsibilities. Ransomware attacks seek to encrypt a Council's data preventing systems from being able to access and process it, whilst charging the Council a ransom to decrypt it. These types of attacks are often in the form of what's called "double extortion", in these cases attackers will also take a copy of the data and threaten to leak or sell it. Where the data contains personal and/or sensitive information about our residents this would put them at risk of identity theft and potentially also targeted themselves by cyber criminals. Our policy follows strong government advice not to pay a ransom.

Denial of Service attacks are still attempted on Council websites and online services. In these cases the attack seeks to overwhelm the service with a huge number of simultaneous requests, this can crash the website preventing residents from being able to access the services they need.

- **Social engineering and phishing** campaigns as a way to access Council systems. These techniques seek to exploit staff and Councillors, in order to gain user IDs and passwords to allow the attackers into our network.
- **Legacy IT infrastructure** and budget constraints can result in unpatched systems and gaps in security coverage.

The nature of the market for cyber attacks is now sufficiently advanced that anyone with an intent to do damage and without the necessary skills can buy the services of sophisticated cyber criminals to target organisations or individuals for them.

We are also seeing the advance of AI being used as a weapon to support cyber attacks and as a tool to strengthen cyber defences. The Council benefits from AI monitoring of our systems and we expect to continue to see further investments in AI and other advanced technologies to continue to keep pace with the advances in threats that we face.

Recent PCC Experience

We cannot ignore these threats or presume that we are not being targeted, the truth is that every day we are repelling attacks. Some examples:

- **Denial of Service attacks** recently our website has been the subject of a regular cycle of denial of service attacks from a pro Russian cyber group
- **Phishing** every day our email filters block around half the emails sent to the Council as they are recognised as either spam or phishing attempts. Despite the technical defences some phishing emails are delivered to staff and Councillors. We have had one incident in the last 2 years where this resulted in an attacker successfully gaining access to a user account.
- **Vulnerabilities exposed by unpatched systems** we recently detected and removed an attack in progress on a server where the attacker was seeking to install their own code into our systems exploiting a vulnerability before it had been patched.

Case Studies and Recent Incidents

Several UK councils have faced major cyber incidents in recent years. For example, Redcar and Cleveland Borough Council endured a devastating ransomware attack in 2020, which reportedly cost over £10 million and disrupted services for months. Hackney Council was also hit by ransomware, which severely impacted housing benefit payments causing financial hardship as well a severe reputational impact and lack of trust in the Council. It also had numerous other impacts such as preventing access to records including those used to respond to searches to allow property sales. The problem created severe delays to all property transactions in the borough for months. Even with good business continuity plans and strong technical defences the impact on services in Plymouth would be profound and long lasting if we fell victim to a similar ransomware attack.

Building Our Cyber Resilience

Addressing cyber risk is not just a technical challenge, it requires a cultural and leadership response too. Our cyber resilience relies in the following factors:

- **User Awareness & Training:** We use the KnowBe4 software to regularly train all staff and Councillors on how to identify and avoid phishing, social engineering, and other threats. Since being introduced just over a year ago our ability to spot and report threats has significantly improved. We call this aspect of our cyber defences our "human firewall".

Leadership and Governance: We provide quarterly reports (as part of the Information Governance reports) to CMT and annual reports to the Audit and Governance Committee. These reports help these groups understand the risk we face, how they can champion cyber security and embed it within organisational culture and priorities.

Incident Response Planning: Working with Delt and our Civil Protection Team we test our response plans and our business continuity plans.

Asset Management: We are investing currently in new tools to help Delt better track what devices are connecting to our systems and who is using them.

Access Controls: We are also working with Delt to ensure the access to systems and data that Councillors and staff have is limited to only that required by their role.

Vendor and Supply Chain Risk Management: Delt check all third-party suppliers carefully and set out suitable security standards to be followed as part of procurement.

Backup and Recovery: On our behalf Delt maintain secure off-site backups and ensure recovery processes are regularly tested and updated.

Network Security: We have a number of technical defences including recently upgraded firewalls as well as a contracted specialist 3rd party monitoring agency looking for threats and advising Delt on emerging threats and vulnerabilities

Monitoring and Threat Intelligence: As well as the 3rd party support to Delt we also subscribe to the notices provided by the National Cyber Security Centre and MHCLG where they are made aware of vulnerabilities that could impact us.

Conclusion

Cyber threats are real and serious – we are effectively in an arms race with attackers, as we find ways to protect our data and systems, they find new ways to attack. Our investment in cyber defence technology and operations has increased 10 fold in the last 6 years and must be anticipated to continue to increase in order to keep pace with the threats we face. Whilst we continue to invest significantly in our technical defences and through training our human firewall, we must consider ourselves still vulnerable to attack and therefore continue to maintain our vigilance and rehearse our business continuity plans.