Empowering Progress and Ensuring Safety

Securing Your Local Authorities From Cyber Threats

Local authorities in the public sector are prime targets for cyber criminals, inherently due to amount and nature of sensitive data they hold and the critical services they provide to our communities. Furthermore, much of this data is also shared between organisations and departments as part of modern governance and improving the delivery of public services.

There is an urgent need for comprehensive cybersecurity measures that local authorities need to implement. Beyond financial losses, cyber incidents can jeopardise the privacy of local citizens, which diminishes the assurance the public places in their local authorities and hinders the delivery of essential services. Furthermore, the interconnected nature of digital infrastructure further amplifies the impact of potential cyber incidents, necessitating a proactive strategy to remain robust in the face of cyber threats.

Cyber Security Failures

In recent years, local authorities within the public sector have faced numerous notable cybersecurity failures that underscore the need for implementing robust security strategies and technologies to protect themselves and their citizens.

In 2023, it was found that UK councils have disclosed nearly 1,500 data breaches in a year alone, with Suffolk County Council as one example having over 600 incidents in the first three quarters of the year.

In the US, the city of Atlanta fell victim to a ransomware attack in 2018, encrypting essential and sensitive data until a hefty ransom was paid for its release. While it may sound relatively simple at a first glance, the consequence of this attack was a significant financial loss, as well as the disruption of key municipal services and other widespread disruptions.

While data breaches are becoming a common, almost daily occurrence nowadays, local authorities have shown strength in disclosing and reporting of cybersecurity incidents. However, with the number and frequency of incidents increasing, and an evolving cyber threat landscape, local authorities should investigate improving their cybersecurity capabilities to prevent the possibility of posed threats and mitigate any attack.

Safeguarding is Imperative

Protecting local authorities against cyber threats involves a multi-faceted strategy. This includes, but is not limited to:

- Robust cybersecurity policies and procedures
- Regular training for all personnel
- Advanced threat detection and response mechanisms
- Investment in secure infrastructure

This, and the existing mechanisms that supplement incident reporting and transparency can significantly improve their protection capabilities.

Achieving Cyber Security Resilience With Sapphire

To ensure resilience against cyber threats, local authorities should approach security holistically, proactively and strategically.

Risk management

Local authorities should conduct thorough risk assessments to identify potential vulnerabilities, threats and the impact of these threats on their operations, and those they support.

Sapphire can help assess the confidentiality, integrity and availability of all critical systems and data and provide structured approaches to risk management using key frameworks such as:

- GovAssure
- NIST Cybersecurity Framework (CSF)
- NCSC Cyber Assessment Framework (CAF)
- ISO 27001

Another essential part of managing risks involves establishing and maintaining a comprehensive inventory of digital assets. This includes hardware, software, networks and data repositories, and understanding the value of your assets can help you better prioritise security measures and align them with the local authority's objectives.

Training and Awareness

A robust security training and awareness program is imperative for improving and maintaining good security posture. Sapphire can create bespoke, tailored training plans that cover a wide array of critical areas, including phishing, password best practices and understanding the importance of data confidentiality, among many others.

Continuous Monitoring

Remaining robust to cyber threats in a constantly evolving digital landscape is a difficult challenge, and doing so requires real-time collection and analysis of security data to detect and respond to threats posed to you.

Sapphire's threat intelligence capabilities use real-time intelligence data from a variety of credible sources, which are embedded into market-leading technology platforms that can supplement your searching, alerting and reporting capabilities. Our managed threat intelligence services can help you stay informed about emerging threats and vulnerabilities relevant to the services you provide.

In addition to this, our Security and Information Event Management (SIEM) solutions can help you analyse log data from a wide array of systems, providing you with a centralised view of automated detection of anomalies or suspicious activities.

Threat Detection and Response

Attacks can happen at any time, even when you're prepared. While it is challenging to predict when new or existing threats emerge, it is important to respond effectively and efficiently.

Sapphire can provide a best-in-class approach to response and containment to any incident, reducing downtime of critical services and limiting damages and costs. Furthermore, our Managed Detection and Response (MDR) service allows you to focus on your core business functions while we keep your digital environments secure and compliant with key frameworks.

Audits and Testing

Conducting regular penetration testing allows you to assess the effectiveness of implemented security measures in your local authority by finding vulnerabilities and observing how they can be exploited.

Sapphire offers a range of penetration tests and analysis services that can cover a wide array of services, including social engineering tests, web and mobile application tests, as well as testing your infrastructure and networks.

Besides, Sapphire can also conduct Breach Attack Simulation (BAS) which can simulate real-world cyber-attacks against your authority in a controlled environment. This allows us to help pinpoint any vulnerabilities that could disrupt your critical services.

Service /Offering	Introductory	Foundations	Intermediate	Advanced
NCSC Guidelines	✓	✓	✓	✓
Standards Compliance Review	✓	✓	✓	✓
Gap Analysis	✓	✓	✓	✓
Security Improvement Planning	✓	✓	✓	✓
Security Awareness & Training	✓	✓	✓	✓
Procedure & Policy Review	✓	✓	✓	✓
Network Configuration Review	✓	✓	✓	✓
Risk Review	✓	✓	✓	✓
IT/OT Asset Discovery	✓	✓	✓	✓
Firewall Security Checkup	✓	✓	✓	✓
Framework Review (CyberEssentials, GovAssure)	✓	✓	✓	✓
Information Security Management	✓	✓	✓	✓
Authentication Review		✓	✓	✓
Business Continuity Planning		✓	✓	✓
Disaster Recovery Planning		✓	✓	✓
Incident Response Planning		✓	✓	✓
Identity & Access Management Review		✓	✓	✓
Threat Assessment		✓	✓	✓
Penetration Testing		✓	✓	✓
Internal/External Audit		✓	✓	✓
Threat Intelligence			✓	✓
Vulnerability Management			✓	✓
CISO as a Service			✓	✓
Third-Party Risk Management			✓	✓
IT/OT Consultancy			✓	✓
MXDR & Endpoint Management				✓
Red Teaming				✓
Breach Attack Simulation (BAS)				✓
SIEM & SOC Advisory Services				✓

To find out more or to speak to an expert contact us today

CONTACT US TO FIND OUT MORE

Or call: 0845 58 27001