SOPHOS
Cybersecurity delivered.

# Cybersecurity for Public Authorities in Scotland

*A Sophos Whitepaper. December 2022*

## The changing face of technology in public authority

Public authorities suffer from an often-unfair reputation for being mired in paperwork and bureaucracy. However, the 129 public bodies in Scotland are digitising at pace and have embraced technology using digital solutions for a variety of online services such as portals and payments systems for citizens, employees and suppliers.

In March 2021 the Scottish government published its strategy for growth in the form of A changing nation: how Scotland will thrive in a digital world[1], in which it emphasised the important role played by digital in all walks of life. It pledged to "rethink the way we work and support a country that balances and sustains economic, social and environmental wellbeing in a secure and resilient way."

The impact of COVID certainly accelerated the trend towards embracing digital, as authorities were forced almost overnight to take all their services online. However, the speed of such deployment against a backdrop of fragmented legacy systems has resulted in potential points of vulnerability for cyber-attacks.

Compounding the problem, authorities typically suffer from an IT skills shortage. They can't afford large teams of highly skilled people to work in IT and they certainly don't have time for proactive threat hunting.

The use of technology though is now, more than ever, critical for the delivery of public services. But as authorities work to roll out the latest hardware and software, they find themselves faced with an uphill cybersecurity battle. Faster technology adoption, tighter budgets, fewer skilled IT people all point to major challenges ahead for public authorities in Scotland.

## How Sophos protects in the public sector

The Health Informatics Centre (HIC) at the University of Dundee extended its data centre into an AWS public cloud environment in order to utilise leading-edge technologies such as AI, Deep Learning and Machine Learning and advance the research projects it supports.

A key challenge for HIC was how it could establish a public cloud-based Trusted Research Environment with equivalent security and protection to an on-premise environment. The HIC Infrastructure team sought to achieve this by building a hybrid cloud solution. "We wanted to take advantage of leading cloud technologies to advance health research projects, while upholding stringent governance and compliance with our existing and ongoing information security standards," Ian Fletcher, Information Security and Governance Manager, HIC.

HIC opted for Sophos Cloud Optix "I think one of the key benefits for HIC is the ability to apply consistent 'guardrails' within the AWS environment to ensure compliance with our required information security standards," said Ian, adding: "With Cloud Optix, we can be confident that we are in constant compliance. We also have peace of mind that with Cloud Optix's proactive 24/7 monitoring in place, we would be alerted should any activity deviate from our applied security standards, and any issues flagged to us quickly."

1 A changing nation: how Scotland will thrive in a digital world

## The changing face of cybersecurity

For cyber criminals, public bodies are becoming more attractive and the sector is coming under regular attack. In December 2020 the Scottish Environment Protection Agency (SEPA) was targeted and according to SEPA the "attack displayed significant stealth and malicious sophistication". SEPA did not pay the ransom, however, it was still counting the costs over 12 months after the attack according to Audit Scotland which stated the agency was still rebuilding infrastructure one year on[2]. SEPA itself revealed that the costs to taxpayers of a cyber-attack have risen to at least £5.5 million[3] and counting.

SEPA grabbed the headlines in Scotland, but it is not the only public body attacked in recent times. In March 2021 the University of the Highlands and Islands was forced to temporarily close 13 colleges and research institutions due to a cyber-attack[4]. In fact, according to the Scottish government, there were a total of 10 public sector cyber incidents in 2021[5].

Ransomware groups are becoming increasingly professional, with well organised company-style structures and ransomware as a service (RAAS) affiliate scheme. It is not the case that threat actors only encrypt data and demand payments for decryption keys, but they increasingly exfiltrate valuable data and threaten to publish, post or sell it as happened with UK social housing group ForViva where data for thousands of citizens was found on the dark web after an attack[6].

According to the Sophos State of Ransomware 2022 report 59% of central and local governments globally were targeted hit by ransomware in 2021. The report also states that overall (in public and private sector industries) there was a 78% increase in ransomware attacks over the course of the year, demonstrating that adversaries have become considerably more capable at executing the most significant attacks at scale.

2 SEPA continues to count cost of cyber-attack
3 Cost of Sepa cyber attack doubles to £5.5m
4 Cyber attack disrupts services at the University of the Highlands and Islands
5 Information on cyber attacks of which public bodies in Scotland have been a victim: FOI release
6 Data stolen as social housing group suffers cyber security attack

## Cybersecurity is a multi-layered threat

The threat posed by ransomware attacks is extremely damaging for public authorities who often handle very sensitive data and are financially responsible for the clean-up. Many authorities are running outdated and fragmented IT infrastructures supported by understaffed IT teams. As a result, in the wake of an attack they are often forced to totally rebuild from the ground up, incurring major financial cost. When balancing usability against cost and protection, it is far wiser to bake security in at the beginning of a process rather than retrofitting it to patch up a vulnerability. However, the speed of deployment often means security can be an afterthought.

In today's world, it is no longer enough to simply deploy antivirus software across networks and expect to be protected. Malware and hacking used to be two different threat landscapes; however, they have merged over the last five years.

Attackers are stealthy – if IT teams don't play an active part in looking for signs of a breach, then cybercriminals can use (often legitimate) tools to enter and move around a network undetected, simply waiting for the right opportunity to strike.

'Hands-on attacks', where the adversary goes interactive within an IT estate, are becoming increasingly common and can unfold at lightning speed, quickly overwhelming staff. If this happens, it's crucial that a public body has the expertise to respond rapidly at any time of day or night and bring in incident response services to assist.

## Barriers to transformative security

As public authorities in Scotland accelerate with their digital transformation plans, it will result in more data being shared across networks and greater commonality of systems. This will result in more points of weakness and more cybersecurity risk as changes take place.

Leadership teams are faced with three key, immediate challenges with digital transformation. First is the complexity of the existing or legacy platforms and software across a fragmented landscape. Second is the requirement to address security and compliance - the immediacy of this requirement can lead to quick fix solutions, which does not help with long-term challenges. The third challenge is a lack of skills with new technologies such as cloud, AI and cybersecurity.

Coping with these challenges is a major headache for IT leaders. Many authorities are streamlining and centralising IT teams. Network managers working a broadening landscape find themselves under increasing pressure.

Public authorities are increasingly looking towards managed service providers to help with these challenges. As the strategic importance of technology increases in line with its complexity, the role of the IT professional is moving up the value chain from implementation expert responsible for building, deploying and maintaining solutions to technology orchestrator responsible for long-term goals and strategy.

## Taking a long-term approach

Security, like insurance, is something you hope you never need, but absolutely must have in place from a compliance perspective and to manage risks. In fact, public authorities would be well placed to work on the assumption that an attack will happen and ensure they have a tried and tested incident response plan that can be implemented immediately to reduce the impact of the attack.

Complicating matters, threats are constantly evolving as criminals try new avenues of attack against the latest security. For instance, phishing is become ever more sophisticated and difficult to spot, especially in environments with high staff turnover, using fragmented IT architecture.

The UK National Cyber Security Centre (NCSC) has made it clear that supply-chain security weaknesses also make organisations highly vulnerable to attack. Authorities should mitigate this risk by reviewing their existing suppliers' cybersecurity measures immediately, and for future contracts, build in security requirements from the start.

Too many cyber breaches are caused by the inadvertent actions of users. Therefore, it is important that users are educated about the cyber risks they face and the safeguards in place to protect them. They should also understand their individual cyber security responsibilities, be aware of the consequences of negligent or malicious actions, and work with other stakeholders to identify ways to work in a safe and secure manner.

## Avoiding breaches – the cybersecurity solutions

Taking a proactive approach to cybersecurity is vital. Public authorities are faced with the choice to either manage IT themselves or outsource. Most do not have the budget, tools, people, and processes in-house to effectively manage their security programme around-the-clock while proactively defending against new and emerging threats. Furthermore, associations who do invest in cyber security solutions often fail to deploy them fully or use them to their full potential – significantly reducing their effectiveness and increasing the likelihood of a successful, but preventable breach.

For an organisation to mount an effective defence against cybercriminals, IT teams often use Endpoint Detection and Response (EDR) or Extended Detection and Response (XDR) tools that monitor and scour the network for suspicious behaviour. However, it takes time and expertise to use these tools effectively and investigate the numerous alerts that require triaging, burdening already overstretched IT staff. Security Incident & Event Management (SIEM) is another often touted solution, but this is even more resource intensive and can end up being very expensive without addressing the need for incident response.

In these circumstances, a Managed Detection & Response (MDR) service is an ideal solution. At Sophos, a human-led threat hunting team works together with AI technology to hunt, detect and respond to suspicious activity 24/7/365, while maintaining an ongoing dialogue with IT staff. More than just a notification service, the team's level of involvement is entirely within an organisation's control – from validating threats and removing all the 'noise' of false positives to carrying out targeted actions on an IT team's behalf. Because these threat hunters are so familiar with malicious behaviour, once detected, the issue is often resolved within the hour.

## ROI Benefit of MDR

Maintaining a 24/7 threat hunting team is expensive. To provide round-the-clock coverage, you need a minimum of five or six cybersecurity staff members working separate shifts. MDR services provide a more cost-effective way to secure your organization and stretch your cybersecurity budget further. MDR services also greatly reduce the risk of experiencing a costly data breach and avoid the financial pain of dealing with a major incident. With the average cost of remediating a ransomware attack in mid-sized organizations coming in at $214 million according to Sophos data, investing in prevention is a wise financial decision.

"Bringing all of our security products under one roof has allowed us to save money and drive efficiency as well," Independent Parliamentary Standards Authority, UK.

Sophos MDR also delivers the capabilities of cloud-based security alert investigation and triage automation solution SOC.OS. The solution consolidates and prioritises high volumes of security alerts from a multiple products and platforms, including third-party telemetry, enabling security operations teams to quickly understand and respond to the most urgent cases flagged.

In fact, this third-party compatibility extends to a wide range of existing cybersecurity solutions, including with endpoint, network, cloud and email security solutions, and identity, SOAR, SIEM, ITSM, threat intel, and RMM/PSA tools. Sophos MDR integrates with existing solutions and an organisation's broader IT environment, streamlining IT operations and elevating defences.

Leveraging bespoke data processing and correlation techniques across this broad set of telemetry, the Sophos MDR operations team is able to quickly understand the who, what, when, and how of an attack, and is capable of responding to threats across customers' entire ecosystems within minutes.

## Conclusion

With a continually changing threat landscape and limited budgets, securing public authorities in Scotland against cyber-attacks requires a collaborative team effort. By working together with your authority, Sophos can provide the best opportunity to minimise security incidents and keep data safe as digitalisation continues apace.

Having a specialist MDR team in your corner at all times – whether they're needed in the middle of the night, at a weekend or during holidays – ultimately provides you with peace of mind, knowing you're doing all you can to keep your service running and your data safe.

Sophos MDR offers different levels of support, giving your authority options around the control you wish to retain or hand over to our team. Plus, there's a wide variety of trusted Sophos security products that work side by side with MDR, all managed from within the Sophos Central platform for total visibility of your estate. You'll be safe in the knowledge that our dedicated security personnel will identify and eliminate threats before they can even become an issue.

Ultimately, what counts is that public authorities fulfil their remit to provide the businesses and citizens of Scotland with services that underpin their continued welfare. If technology is a growing part of achieving that ambition, cybersecurity is fundamental to making it viable. As in many other sectors, public authorities must adapt to the acceleration of cyber-risks - but without panicking. Being a target is now a fact of life, but becoming a victim is not.

To find out more about cybersecurity expertise and solutions in the public sector in Scotland:

Learn More or Request a Call



2022-11-30 (WP-NP)

SOPHOS