SOCURA

Cyber Security in the Public Sector

“Only by ensuring that cyber attacks neither disrupt our core functions, nor erode vital trust and public confidence can we use the full potential of cyber as a lever to protect and promote our interests in a world that is being fundamentally and rapidly reshaped by technology.”

STEVE BARCLAY, CHANCELLOR OF THE DUCHY OF LANCASTER AND MINISTER FOR THE CABINET OFFICE

FOREWORD:

Building a cyber resilient public sector

In 2020 residents in Redcar & Cleveland couldn't access key services or seek social care advice. They couldn't make online appointments or look at planning documents for many weeks after the council's computer systems and website came under attack. Similarly in Hackney, essential council tax, benefits and housing services for residents were left devastated after a ransomware incident.

More recently another target, Gloucester City Council, had their systems breached via an email sent to a council officer, which was later linked to threat actors operating out of Russia. Six months on from the attack, the council was still working to get all its services back to normal.

Despite the relatively small sizes of these organisations, the impact on critical public services was disproportionate and acute. These attacks were not an anomaly, but part of a significant upward trend.

In fact, the future looks ominously bright for threat actors. Fundamental shifts in computing, including the rise of cloud services and the 'Internet of Things,' will exponentially drive growth in big data as companies gather more and more data from more and more devices. As Marc Goodman, author of Future Crimes, said *"Criminals will have an ever-expanding pool of targets from which to choose ... Every gigabyte you store is a gigabyte at risk*[1]*"*.

With UK councils targeted with an average of 10,000 cyber attacks every day since the beginning of 2022[2], building a cyber resilient public sector is becoming more important than ever before.

Andrew Kays, CEO

[1] Goodman, "Criminals deftly exploit the data deluge."

[2] Open Access Government - Why we need a cyber-resilient public sector

Contents

Protecting the functions and services on which we all depend

"Government organisations are routinely and relentlessly targeted [for cybersecurity attacks]: of the 777 incidents managed by the National Cyber Security Centre between September 2020 and August 2021, around 40% were aimed at the public sector. This upward trend shows no signs of abating."

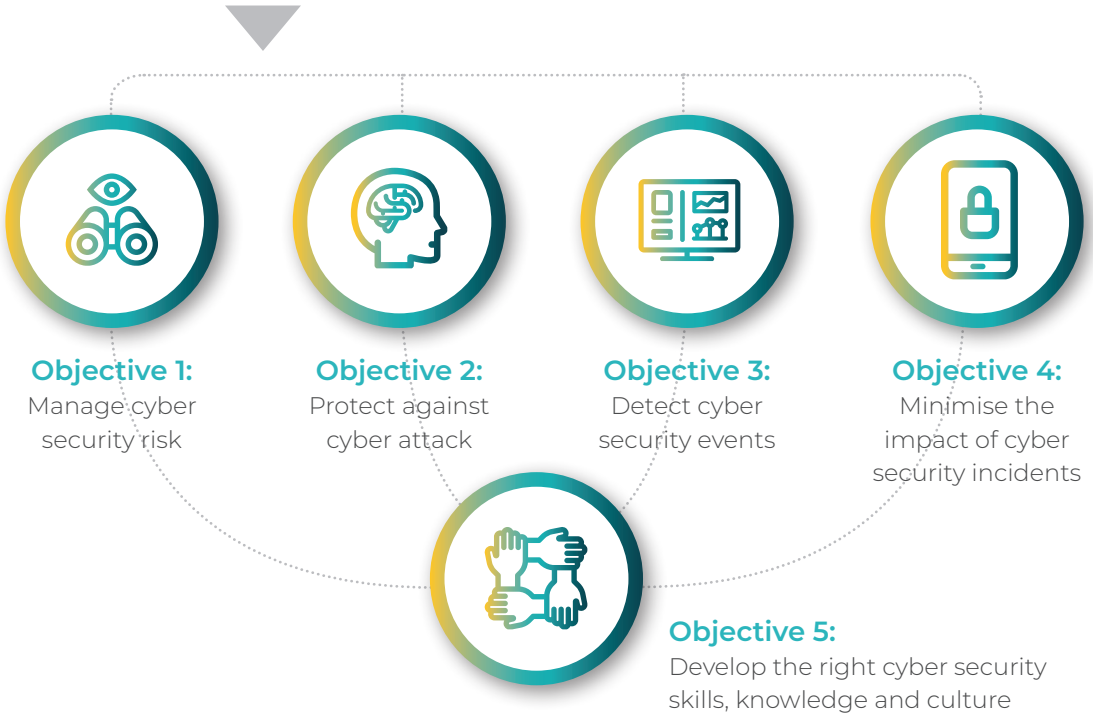
Government Cyber Security Strategy – Ministerial Foreword

Why is the public sector such an attractive target for threat actors? It's partly due to the vulnerability caused by outdated and legacy systems, but more than that, it's the lure of public sector data. Cyber criminals are looking to exploit a treasure trove of personal data for identity theft, financial fraud, account takeovers, or to create spear phishing emails and social engineering attacks that lead to ransomware.

This data also has value. If threat actors were to steal thousands of credit card details by hacking a private organisation such as a bank or online retailer, they'd get a certain price per record when auctioned on the dark web. Now consider they were to attack an NHS Trust and steal medical information, their profit would most certainly be significantly higher. And that's not taking into account the amount they could extort from the targeted Trusts themselves.

Strengthening our countries cyber defences is vital if we are to guard our citizens personal information, and protect the functions and services on which we all depend. As a nation we have made great progress, ranking fifth in The Global Cybersecurity Index[3], but there is much more to do.

This paper looks in more detail at the Government Cyber Security Strategy, and more specifically the underpinning National Cyber Security Centre's (NCSC) Cyber Assessment Framework (CAF). We'll consider where organisations may face challenges and suggest how these could be overcome.



[3] The Global Cybersecurity Index, published by ABI Research and ITU

Objective 1: Managing cyber security risk

Effective cyber security risk management processes, governance and accountability enable the identification, assessment and management of cyber security risks - at both the organisational and cross-government level.

The premise of this objective is, that if a public sector organisation is to effectively manage cyber security risk, they will firstly have to be able to identify, assess and understand them. There are two clear themes that stand out here; asset management and accountability, let's take them one at a time:

Asset management

The foundation of this lies in the visibility and understanding of assets, their vulnerabilities, and the threat to them, whether internal to an organisation or coming from the supply chain.

Anyone who has worked in IT in the public sector, or outside, knows that this is not as easy as it perhaps sounds, and an already difficult task has become tougher as councils, hospitals and schools alike explore new technologies to help drive efficiency, keep connected and cut costs. A digital revolution in the public sector is underway, but there's a growing gap between digital maturity and cyber maturity.

The challenge has been compounded as the UK Government spent millions expanding its digital repertoire in response to the pandemic. In keeping with most other sectors, the civil service has seen a high level of hybrid homeworking long after the crisis has passed. A progressive step, but one that requires an even greater commitment to technological innovation — as well as a deep understanding of cyber security concerns.[4]

In our own poll conducted earlier this year, in partnership with Surveys in Public Sector, 51% of respondents saw challenges arising from 'managing vulnerabilities from legacy systems and software'[5]. Organisations will need to overcome known legacy and data issues in a situation where IT assets are not always catalogued or risk assessed, and where the sheer size and complexity of the supply chain, including nuances of data access and privileges, combined with how data is increasingly moving in and outside of the system via third-party vendors, has increased the likelihood of vulnerabilities.

SOCURA INSIGHT

Organisations could consider using IoT Security services that have been designed to identify and classify all IoT and OT devices on the network. By using Machine Learning and Next Generation Firewall technology, newer services can even identify devices never seen before.

There's also Managed Vulnerability Scanning (MVS) services that can help you to identify, prioritise and remediate vulnerabilities in your business-critical assets, whether on-premises or in the cloud. By layering MVS data into investigations, your cyber teams capabilities are enhanced with further context. This is more important than ever, with vulnerabilities evolving all the time as systems are updated, and new attack techniques becoming available.

[4] Open Access Government - Outdated government tech increases cyber threats
[5] Survey in Public Sector - Managing Cyber Threats in the New Digital Era

Accountability

The goal is clear accountability and robust assurance that ensures risk owners are aware of the risks they have the responsibility to manage, and that they are doing so appropriately.

The challenge here is that within the public sector there is not always a clear chain of command in cyber security, or enough knowledge across management boards, which can lead to a lack of ownership of the issue. Speaking to researchers writing a government report[6], one digital transformation manager in the public sector spoke of how their Board assumed that the data protection officer, a different individual, was responsible for overseeing cyber security at a senior level. However, this person was overloaded with other, non-cyber work.

The same publication reports that a quarter of public sector organisations have just one staff member responsible for cyber security, and the percentage of public sector organisations outsourcing basic security functions such as firewalls, user privileges and backing up data, for instance, far outweighs that of the private sector[7]. In a 2022 study by Deloitte[8] the third biggest barrier that respondents faced when responding to cyber security challenges was 'Inadequate cyber security staffing' (46%), likely impacted by number two, 'Inadequate availability of cyber security professionals' (50%).

The common theme here is a lack of internal resources and control. The technology is available, but only if the public sector is willing to continue putting up with the 'technology debt' it's accruing through its overdependence on outdated internal tech and external cyber security solutions, and all of this makes the lines of accountability ever more blurred. Perhaps this is why a recent Gartner survey found that 75% of organisations are pursuing security vendor consolidation, with 65% choosing to do so to improve their risk posture[9]. Whatever approach is taken, roles need to be more clearly defined, responsibilities outlined with no ambiguity, and agreed channels for communicating and escalating risks to ensure that decision makers have the visibility required to make effective decisions. Most crucially, it requires clear and transparent accountability right up to the Executive Board, to ensure that decision makers are informed and empowered to express their organisation's risk position, and be held accountable for their risk decisions.

It's worth noting that The Department for Digital, Culture, Media & Sport's Cyber Security Breaches Survey series[7] has also consistently highlighted the importance of Board engagement with cyber security "There needs to be more visible ownership … It has been moved around quite a few times. It should be the whole Board, not just one individual."

The message couldn't be clearer; increased risk, coupled with a rise in demand for digital services, means that cyber security should no longer be just a concern for the IT department; Information and cyber security must now be a Board priority.

SOCURA
INSIGHT

Consolidating security tools and suppliers can help you to gain control and reduce risk, look for a partner that can work with you to understand your entire cyber landscape. XDR solutions offer good opportunity for consolidation.

The NCSC has plenty of guidance that can be used by public sector bodies, one of which is the 'Board Toolkit', that has a selection of resources designed to encourage essential cyber security discussions between the Board and their technical experts.

[6] The Department for Digital, Culture, Media and Sport - Cyber security skills in the UK labour market 2021
[7] GOV.UK - Cyber Security Breaches Survey 2020
[8] Deloitte - NASCIO Cybersecurity Study 2022
[9] Gartner - Gartner Survey Shows 75% of Organizations Are Pursuing Security Vendor Consolidation in 2022

Objective 2:
Protecting against cyber attacks

Understanding of cyber security risk informs the adoption of proportionate security measures with centrally developed capabilities enabling protection at scale.

At the heart of this objective is the clear link between the assessment and management of risk, and the protective stance that public sector organisations take. While it will never be possible to protect against all attacks, those accountable should be able to demonstrate that they have considered risks, and responded accordingly. New thinking in this area revolves around a change in mindset and approach.

A change in mindset

How can organisations reverse the growing gap between security investment and effectiveness? Traditionally, cyber security has focussed on preventing intrusions, defending firewalls, monitoring ports, and so on, and these are certainly a good first step. Similarly, prompt patching, anti-malware on end-user devices, regular end-user training, network segmentation, strict user access controls and more can often be enough to repel commodity threats. But, the evolving threat landscape calls for a more dynamic approach.

As Ed Powers writes in the WSJ Risk & Compliance Journal: "The reality is that cyber risk is not something that can be avoided; instead, it must be managed. By understanding what data is most important, management can then determine what investments in security controls might be needed to protect those critical assets."[10]

Consider taking simple steps such as two-factor authentication and encryption for sensitive data. For extremely sensitive information such as census data, have that data decentralised, with as much of it offline as possible, and with very tight controls and accesses. "Forget convenience and focus on security", says security veteran John Watters.[11]

Public sector organisations should consider assessing the sensitivity levels of the data they hold and protecting as appropriate. Public information such as swimming pool timetables should be stored differently than medical records. Even more sensitive data, like biomedical details, deserve the highest tier of protection.

[10] Ed Powers and Mary Galligan, "The pursuit of cybersecurity," Risk and Compliance Journal, July 27, 2015,

[11] Deloitte interview with Interview with John Watters, October 19, 2015

A new approach

Today, the threat from sophisticated cyber crime groups, hackers-for-hire and occasionally even nation state actors means that IT security leaders need to go one step further in their efforts; going beyond prevention alone, to also focus on swift detection and response.

Security breaches will occur, the only variable factors are timing, severity and how quickly you can respond, so modern cyber security thinking involves building defence in depth and focusses around three fundamental capabilities: being secure, vigilant, and resilient.[12] We've covered 'secure' in some detail on the previous page so now lets look at 'vigilance, we'll look at 'resilient' later in the report

To address cyber threats effectively, organisations need a Cyber Threat Intelligence (CTI) capability that will help them rapidly identify, detect, and respond to threats.

Active Cyber Defence is an NCSC programme that seeks to 'protect the majority of people in the UK from the majority of the harm caused by the majority of the cyber attacks the majority of the time'. It's made up of a growing number of capabilities, one of which is the Cyber Threat Intelligence Adaptor, allowing authorised organisations to receive a high-quality, contextually rich, cyber threat intelligence feed from the NCSC.

By combining this threat intelligence with your own security telemetry, your cyber teams should be able to focus on what matters most to them, intelligence with relevant value.

SOCURA
INSIGHT

Remember, a regularly updated inventory is essential to accurately catalogue assets. You can't protect what you can't see.

Then collect and centralise as much security telemetry from these assets as possible, and keep it hot and searchable for at least 12 months so you can instantly and retroactively match newly discovered indicators of compromise against your entire historical telemetry dataset.

[12] Deloitte - Changing the game on cyber risk 2017

Objective 3: Detecting cyber security events

Comprehensive monitoring of systems, networks and services enable cyber security events to be managed before they become incidents.

Here the goal is to build on the foundation of risk management (objective 1), and the corresponding protective measures (objective 2), and develop a capability to detect cyber security events, so that risks can be mitigated before they become incidents that critically impact services. We see a number of factors to think about here: effective monitoring with visibility across data sources; reducing complexity; and the resulting alerts fatigue; and improving detection at scale through better information exchange.

Effective monitoring

Public Sector organisations need the capability to monitor systems, applications and endpoints, and with 79% of respondents in our survey saying they had already put endpoint protection, detection and response procedures in place[13], a good start has been made. However, address threat detection and response across different parts of the IT estate in a siloed manner and you're likely to miss something.

Today's siloed tools force analysts to pivot from console to console to verify threats, resulting in missed attacks. Analysts face a deluge of alerts – 11,047 alerts a day on average[14]. Visibility gaps are common, making it harder for analysts to correlate and prioritise events and alerts. Exhausted analysts and longer mean time to respond (MTTR) will usually follow. Security teams need help keeping up with an endless backlog of alerts.

A lack of orchestration and automation is often part of the problem. It opens the door to extra complexity, human error, slow and manual response, this in turn results in attacker dwell time being lengthy enough for the threat actor to achieve their objectives (lateral movement, encryption, ransom demands, data destruction, data exfiltration, and extortion).

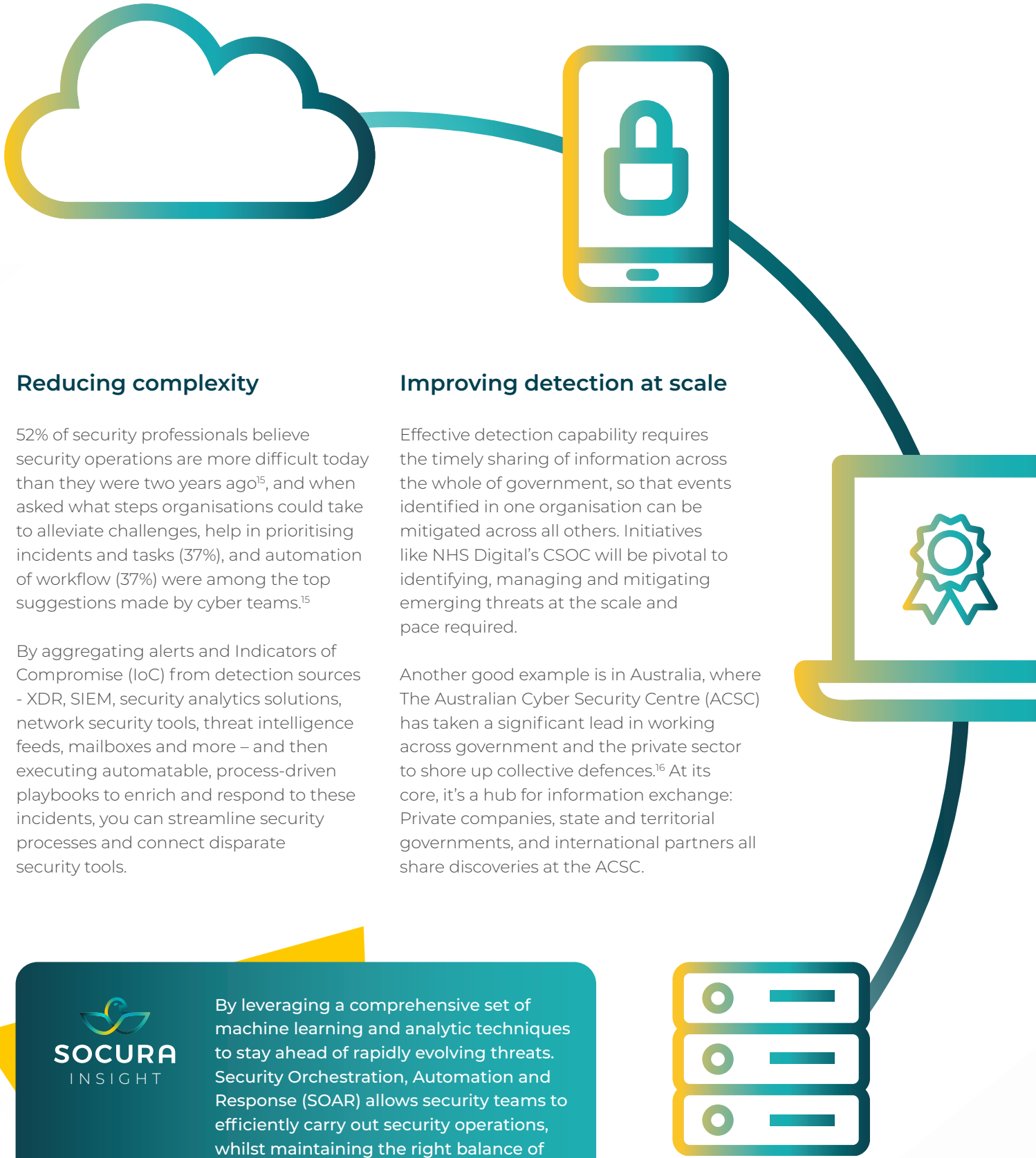
SOCURA
INSIGHT

Visibility, context, and control is the name-of-the-game, stitching together events across cloud, network, and endpoint layers for comprehensive insight — an approach known as Extended Detection and Response (XDR). XDR accelerates investigations by providing a complete picture of every threat and automatically revealing the root cause.

Intelligent alert grouping and alert de-duplication simplify triage and reduce the experience required at every stage of security operations. Tight integration with enforcement points lets analysts respond to threats quickly.

[13] Survey in Public Sector - Managing Cyber Threats in the New Digital Era

[14] Forrester Consulting - 2021 State of SecOps Report,



Reducing complexity

52% of security professionals believe security operations are more difficult today than they were two years ago[15], and when asked what steps organisations could take to alleviate challenges, help in prioritising incidents and tasks (37%), and automation of workflow (37%) were among the top suggestions made by cyber teams.[15]

By aggregating alerts and Indicators of Compromise (IoC) from detection sources - XDR, SIEM, security analytics solutions, network security tools, threat intelligence feeds, mailboxes and more – and then executing automatable, process-driven playbooks to enrich and respond to these incidents, you can streamline security processes and connect disparate security tools.

Improving detection at scale

Effective detection capability requires the timely sharing of information across the whole of government, so that events identified in one organisation can be mitigated across all others. Initiatives like NHS Digital's CSOC will be pivotal to identifying, managing and mitigating emerging threats at the scale and pace required.

Another good example is in Australia, where The Australian Cyber Security Centre (ACSC) has taken a significant lead in working across government and the private sector to shore up collective defences.[16] At its core, it's a hub for information exchange: Private companies, state and territorial governments, and international partners all share discoveries at the ACSC.

SOCURA INSIGHT

By leveraging a comprehensive set of machine learning and analytic techniques to stay ahead of rapidly evolving threats. Security Orchestration, Automation and Response (SOAR) allows security teams to efficiently carry out security operations, whilst maintaining the right balance of machine-powered security automation and human intervention.

[15] Devo - SOC Performance Report 2022

[16] Washinton Technology - Cybersecurity as chess match: A new approach for governments

Objective 4:
Minimising the Impact of Cyber Incidents

Cyber security incidents are swiftly contained and assessed, enabling rapid response at scale.

Think of this in medical terms, prevention is clearly better than cure. But what if, despite vaccines, you get the flu? Your body's response kicks in, increasing your body temperature to create an inhospitable environment for the virus. The identity, source, and intent of the threat are irrelevant, the focus is on isolating and attacking it.

Effective incident response

Similarly, an organisation's resilience to a cyber attack, the ability to contain damage and mobilise resources to minimise the impact - can be what saves it when disaster strikes. How quickly an organisation can detect and then quarantine intrusion can determine the extent to which it can minimise further damage, neutralise threats, and recover.[17]

However, many organisations don't recognise the importance of in-house incident response skills. When asked how important it is to have these skills, just 34% of public sector organisations considered these skills to be essential[17], this number really ought to be a lot higher.

In a previous section we talked about the three fundamental capabilities needed to build defence in depth: being secure, vigilant, and resilient, this is where resilience comes in. Resilient organisations will have appropriate cyber security incident response plans in place. Plans that clearly set out how and who will respond to an incident, how they will make sure threats are quickly contained, how they will recover, restoring business as usual operations as quickly, and with as little disruption as possible, and importantly, how the organisation will learn from the incident, to understand the root cause and prevent it from happening again.

SOCURA INSIGHT

Don't wait until an incident happens to learn that you're not properly prepared to cope with it. Simulate cyber incident scenarios like a data breach, denial-of-service attack, or malware on a network, to gauge your organisation's speed and readiness, and give teams a chance to practice their responses. These kind of exercises present a safe way to establish the procedures, communication and coordination needed to manage a potential crisis.

[17] The Department for Digital, Culture, Media and Sport - Cyber security skills in the UK labour market 2021

Objective 5:
Developing the right skills, knowledge and culture

Sufficient, skilled and knowledgeable professionals fulfil all required cyber security needs - extending beyond technical cyber security experts to the breadth of professional functions that must incorporate cyber security into the services they provide - all underpinned by a cyber security culture that promotes sustainable change.

We see two distinct considerations here: the skills of the cyber teams themselves, and the knowledge of the users that those cyber teams support.

People in the public sector

From librarians to paramedics, to a local headteacher, there are more than 300 different occupations and around 5.4 million people reported to be working in the UK public sector[18].

Many employees simply do not have the skills or knowledge to recognise security threats when they are targeted by sophisticated cyber criminals, and training can be difficult. When asked about the greatest challenges whilst managing cyber security within their organisations, 'Lack of or insufficient education for users about threats' (46%) was a common answer[19]. With diversified malicious threats and limited internal resources, it is perhaps difficult to ensure staff keep up-to-date with threats that they have to be aware of.

And when it comes to cyber teams themselves, the sector has been facing something of an existential crisis. The need for cyber security professionals across various disciplines has soared. Many of these roles have been newly created, and training is failing to catch up with the surge in demand. Employers sometimes exacerbate the problem by failing to cast the net wide enough when looking for new recruits. The result? A headline shortfall in cyber security professionals of just over 2.7 million[20], including hundreds of thousands in Europe.

It's therefore a challenge that affects employers across all sectors in the UK today. But in the public sector the problem is compounded by the struggle to compete with the private sector. Attracting the brightest and best therefore becomes that much harder when pay scales are significantly below market rates.

SOCURA
INSIGHT

Firstly organisations should ensure their employee onboarding plans, for all types of employees, involve training to make sure they are equipped with the right knowledge to be able to identify possible threats.

Secondly, seek to build a culture of trust and empowerment, where employees feel comfortable reporting security-related incidents, accidents, or mistakes to IT and management.

And when it comes to your cyber teams remember, it may not always be possible to find candidates for cyber security roles with the exact experience you desire. Look further afield for expertise and experience, nurture and train people and teams. Augment capability to gain from the economies of scale of third-party cyber organisations.

[18] Office for National Statistics – Who Works in the Public Sector
[19] Survey in Public Sector - Managing Cyber Threats in the New Digital Era
[20] (ISC)² - Cybersecurity Workforce Study 2021

What Happens Next?

The public sector is certainly not alone in experiencing the challenges we've discussed. Many organisations struggle to gain full visibility and control of their IT assets. They're also impacted by an ever-expanding digital infrastructure to attack, security tool sprawl, the growing expertise of attackers and cyber security skills shortages. But the public sector has witnessed an uptick in attacks, with 18 incidents in the country requiring national-level coordination to mitigate the malware from systems, including attacks on a supplier to the country's national emergency helpline, and a water supply company at South Staffordshire.[21]

A commitment to best practices - as outlined in Cyber Essentials Plus and the Data Security and Protection Toolkit (DSPT) is important to provide a baseline of good security to keep threats at bay, however it's the focus on cyber resilience of 'specified essential functions' that distinguishes the CAF from a set of generic good cyber security practices.

The CAF collection is written primarily in terms of outcomes to be achieved rather than a compliance checklist. There will often be a number of different ways of achieving the specified CAF outcomes, so what are the steps that need to be put in place to drive vital change?

Understand what assets your organisation holds - A regularly updated inventory is essential to accurately catalogue assets. You can't protect what you can't see.

Bridge the maturity gap – Roles need to be more clearly defined, responsibilities outlined with no ambiguity. Engagement from strategic senior level leadership is needed to drive information security maturity.

Good cyber hygiene - Prompt patching, anti-malware on end-user devices, regular end-user training, network segmentation, strict user access control can be enough to repel commodity threats.

Collect and centralise security telemetry - Invest in services that can analyse telemetry and spot anomalous patterns indicating unauthorised activity. These services should be capable of acting upon detections in near real-time and containing confirmed threats.

Defend as One - Leverage the cyber community and partners to defend-as-one. Cyber is now a recognised "team sport" and requires collaborative working.

Build defence in depth - The threat from sophisticated cyber crime groups, hackers-for-hire and occasionally even nation state actors means IT security leaders must go one step further in their efforts. That means going beyond protection, to detection and response.

[21] National Cyber Security Centre cyber threat report 2022.

The Value of MDR

This is where Extended Detection and Response (XDR) and Managed Detection and Response (MDR) come in. MDR is increasingly favoured, as building and manning a 24/7 Security Operations Centre (SOC) in-house is hard to justify from a cost perspective. Organisations can instead utilise the economies of scale that a specialist provider offers, and the enhanced visibility they have into multiple customer environments.

For the Public Sector, MDR offers:

24/7 threat detection and response across remote, endpoint, network, cloud and OT environments.

An extension of your security team, freeing up in-house resource to be more strategic.

Rapid response to mitigate threats before they have had a chance to impact the organisation.

Swift detection and containment provides an extra layer of defence, because prevention can't catch everything.

However, in a fast-growing market, not all MDR services are created equal. Many, for example, are limited by the amount of data they can store, retain and analyse, which can impact their efficacy. Here are three questions to ask of a prospective vendor:

1. **How much security data do you collect, and is this cost-constrained?** Telemetry must be collected from every asset/device, and across all parts of the IT infrastructure (including IaaS, PaaS, SaaS, endpoints, firewalls, email, directory services, DNS, Proxies, VPN, etc). Data should go back a year for maximum visibility.

2. **By how much can you reduce attacker dwell time?** Modern threat actors often move fast. You need to reduce dwell time from days or hours to minutes through threat hunting, automated containment actions, and pre-approved playbooks.

3. **How closely will you work with my existing security team?** The best providers will work seamlessly as an extension of your in-house team, with a dedicated security analyst and customer success manager.

If you would like to find out more about how we can help you, **please contact the team at hello@socura.co.uk**