

Scottish Cyber Activity Report 2026



Scottish
Cyber
Coordination
Centre



Scottish Government
Riaghaltas na h-Alba

Contents

Foreword	3
1. Introduction	5
1.1. The Scottish Cyber Activity Report	5
1.2. The Scottish Cyber Coordination Centre	6
1.3. The Scottish Public Sector	7
2. Incidents	8
2.1. Threat Intelligence and Vulnerability Coordination	8
2.2. Incident Preparedness	9
2.2.1. Preparedness in numbers	9
2.3. Incident Response	11
2.3.1. The Incident Coordination and Response Workstream	11
2.3.2. Incidents in numbers	11
3. Exercising	13
3.1. Exercising in numbers	14
3.2. Exercising Themes	15
4. Looking Ahead	16
4.1. Themes & Lessons	16
4.2. Conclusion	21
5. References	22

Foreword

The cyber threat to Scotland's public sector is real, it is growing, and it demands our collective attention. This first Scottish Cyber Activity Report sets out, in evidence, the scale and nature of that challenge. It is a report I am proud to introduce, because it represents something Scotland has not had before: a comprehensive, data-driven assessment of cyber activity across our public sector, drawn from the work of the Scottish Cyber Coordination Centre (SC3) and the organisations we serve.

The picture it paints is honest. Since 2018, SC3 and the Scottish Government has coordinated the response to 183 cyber incidents across the sector, with 43 in 2025 alone. Ransomware remains the most prevalent and disruptive threat, and the under-reporting of incidents continues to limit our ability to respond collectively. At a UK level, the National Cyber Security Centre reports that nationally significant incidents have more than doubled in a single year. Scotland is not immune to these trends. Our public sector holds vast quantities of sensitive data, delivers services on which millions of people depend daily, and operates in a threat environment that grows more sophisticated by the month.

Yet this report also gives cause for confidence. 97% of organisations now receive actionable threat intelligence. The vast majority have incident response plans in place and are investing in cyber resilience training. Engagement with SC3's exercising programme is growing, and the quality of preparedness across the sector is measurably improving. These are not small achievements. They reflect years of sustained effort by dedicated professionals across every part of the public sector.

There is, however, more to do. The lessons in this report are clear: business continuity plans must be scoped for cyber scenarios; communications resilience needs to be treated as a core capability, not an afterthought; incident response capacity across the sector remains uneven and the lessons we identify from incidents must be shared and acted upon with more immediacy. When the same lessons recur across incidents separated by years, we are not failing to learn, we are failing to implement. That must change.

The refreshed Strategic Framework for a Cyber Resilient Scotland 2025–2030 sets out the vision for the years ahead, and SC3 is committed to driving delivery against its outcomes. No single organisation can tackle this challenge alone. Resilience comes from working together, sharing information, and building capacity across the country. That collaboration is already happening, and it is one of Scotland's genuine strengths.

Knowing is half the battle. This report provides the knowing. The doing - the investment, the governance, the exercising, and the collective commitment to improvement, is the work ahead of us. I am confident that Scotland's public sector is ready to meet it.

**Alan Gray**

Head of the Scottish Cyber Coordination Centre
Deputy Director, National Cyber Security and Resilience Division
Scottish Government

1. Introduction

1.1. The Scottish Cyber Activity Report

The Scottish Cyber Activity Report (SCAR) is an annual publication by the Scottish Cyber Coordination Centre (SC3) which examines cyber activity – namely cyber incidents and cyber exercises – across Scotland’s public sector. The report provides an evidence-led, broad view of the incidents experienced across the sector, supported by analysis that identifies recurring themes and highlights identified lessons. SCAR’s purpose is to offer practical insight into what the sector is facing, how well-prepared organisations are, what is working effectively, and where further improvement is required.

SCAR also explores cyber exercising, an increasingly important component of cyber resilience within the public sector. Drawing on insights gathered through SC3’s coordination role, the report reflects on lessons identified from a wide programme of exercises delivered across the sector and considers how exercising is strengthening preparedness, improving decision-making, and supporting coordinated incident response.

As services across the Scottish public sector continue to digitise, the cyber threat landscape evolves alongside them. Greater connectivity and growing reliance on digital systems bring substantial benefits to the people of Scotland, but they also broaden the potential impact of cyber incidents. From service disruption to data compromise, the threats facing the sector are becoming more complex, more persistent, and more capable of causing operational and societal harm.

SCAR is underpinned by several key data sources:

- **Internal SC3 data** provides detailed tracking of cyber incidents and cyber exercises across the sector.
- **Findings from the Cyber Resilience Assessment (CRA)** contribute a comprehensive evidence base, drawing on responses from 181 organisations and offering insight into capabilities, practices, and overall preparedness across the Scottish public sector.
- **The National Cyber Security Centre’s Annual Review**¹ provides context for Scotland’s public sector in the wider UK scene
- **The Cyber Security Breaches Survey 2025**² details threats faced across the UK and how these compare to Scotland’s public sector

1.2. The Scottish Cyber Coordination Centre

The Scottish Cyber Coordination Centre (SC3) is the focal point for cyber security and resilience across Scotland's public sector. Established in 2022 following the Scottish Government's Cyber Resilience Strategy, SC3 sits within the Scottish Government's Digital Directorate and operates as the central coordination function for cyber threats, incidents, and resilience support to the public sector. In 2025, the Scottish Government published a refreshed Strategic Framework for a Cyber Resilient Scotland 2025–2030,³ setting out seven outcomes to guide the country's approach to cyber resilience over the next five years.

SC3 holds direct ownership of Outcome 2, that Scotland has the capability and capacity to respond effectively to cyber incidents, encompassing the national framework for incident response, coordination, and recovery of essential digital public services. SC3 also carries significant delivery responsibility across Outcome 4, which focuses on ensuring public sector organisations effectively manage their cyber risks. This includes supporting organisations to embed cyber resilience into governance, strengthen incident readiness, build professional capability, improve incident reporting, and secure legacy systems. Taken together, these responsibilities position SC3 not only as the national operational coordination centre for cyber incidents, but as a key driver of the maturity of cyber resilience across Scotland's public sector.

SC3 operates across five core workstreams:

- Standards and Insights
- Threat Intelligence
- Vulnerability Management
- Incident Coordination
- Cyber Exercising

SC3's mission is to strengthen public sector cyber resilience through coordination, shared learning, and data-driven prioritisation. It works closely with the National Cyber Security Centre (NCSC), Police Scotland and a broad range of sector partners to ensure that Scotland's public sector is informed, prepared, and able to respond effectively when incidents occur. Its role is not regulatory or enforcement-based, instead SC3 is a trusted coordination body, working on the basis of collaboration and shared learning. The SC3 Strategic Plan sets out the operating principles and objectives for the centre.⁴

1.3. The Scottish Public Sector

SC3's remit covers the breadth of the Scottish public sector consists of approximately 180 public bodies spanning a diverse range of functions and services. These organisations fall into several broad categories:

- central government, executive agencies, and non-departmental public bodies
- local authorities
- health boards
- emergency services
- universities and colleges
- publicly owned corporate bodies
- other organisations such as valuation joint boards and inquiries.

This breadth reflects the reality that cyber risk does not respect organisational boundaries or sectoral silos. Each part of the sector carries distinct cyber risk. A cyber attack on a local authority can disrupt housing, care services, planning, and primary and secondary education. An incident affecting a health board can compromise patient safety and clinical systems. An attack on a university or college disrupts learning, research, and the management of sensitive student data. Across the emergency services, digital disruption can have immediate consequences for public safety. The sector collectively manages vast quantities of sensitive personal data, operates services on which the public depends daily, and plays a foundational role in the confidence and resilience of Scottish society. Its cyber resilience is therefore a matter of national importance.

2. Incidents

The Scottish public sector experiences cyber activity regularly. Between 2018 and early 2026, SC3 managed, coordinated or engaged in responses to 183 incidents, ranging from low impact denial of service attacks to widespread ransomware campaigns and major network compromises. These incidents have affected organisations across every sector: local authorities, health bodies, central government, education, and the private suppliers that the public sector services depend. Each incident has generated learning and collectively, they paint a picture of Scotland's cyber maturity and the capabilities required to respond effectively.

This section examines the threat landscape, preparedness across the sector, and the key lessons emerging from incident response operations.

2.1. Threat Intelligence and Vulnerability Coordination

Effective incident response begins long before an attack occurs. It depends on organisations having timely access to threat intelligence, the tooling to detect threats, and the capacity to act on warnings when they arrive.

SC3 distributes threat intelligence through two primary channels. CREW (Cyber Resilience Early Warning) notices and TIPR (Threat Intelligence Priority Reporting) In the last year, SC3 issued 60 CREW notices and 23 TIPR notices, reaching hundreds of recipients across the sector. Additionally, SC3 has published 83 reports and triaged 119 vulnerability disclosures, providing a steady stream of information to help public sector organisations understand and mitigate emerging threats.

The impact of this work is evident in the Cyber Resilience Assessment. Of the organisations surveyed, 97% reported that they receive threat intelligence from SC3 or other sources, with 86% subscribed to the SC3 daily threat report, suggesting a high level of uptake and value from the services SC3 provide in relation to threat intelligence. However, receipt of threat intelligence is only the first step. The CRA found that 89% of organisations use at least one tooling option for threat detection which is a significant capability, whilst 91% confirmed they can act on threat intelligence received. This suggests a generally mature level of threat intelligence integration across the sector, though the gap between those receiving intelligence and those able to act on it should not be overlooked.

Vulnerability coordination is equally important. SC3's work to identify and disclose vulnerabilities affecting multiple organisations has prevented exploitation and enabled the sector to patch in a coordinated manner. This work is particularly critical in the context of supply chain risk, where vulnerabilities in widely deployed software can affect hundreds of organisations simultaneously.

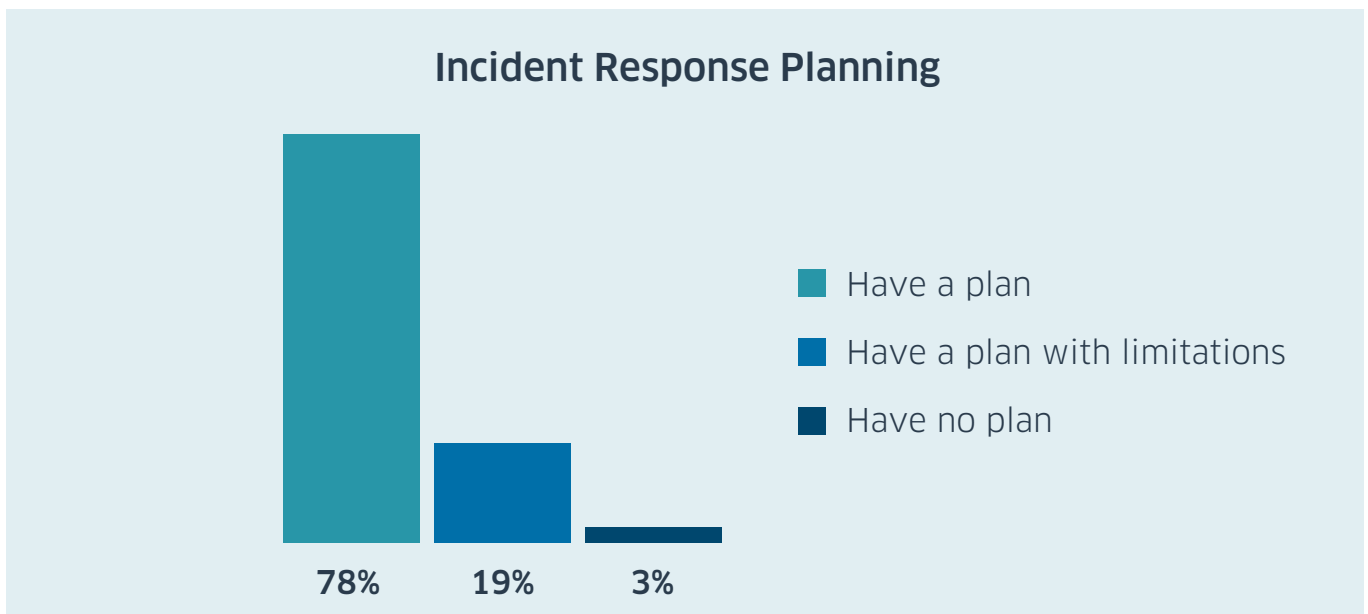
The above shows the level of preparedness for the sector is strong when identifying threats and demonstrates that organisations are not only receiving and consuming intelligence but are also increasingly equipped with the tools or means and operational capacity needed to detect, prioritise, and act on those threats. Together with SC3’s vulnerability coordination work, this reflects a sector that is building resilience proactively rather than reactively, ensuring that early warning and threat detection are in place to combat the ever-increasing cyber activity seen across the sector.

2.2. Incident Preparedness

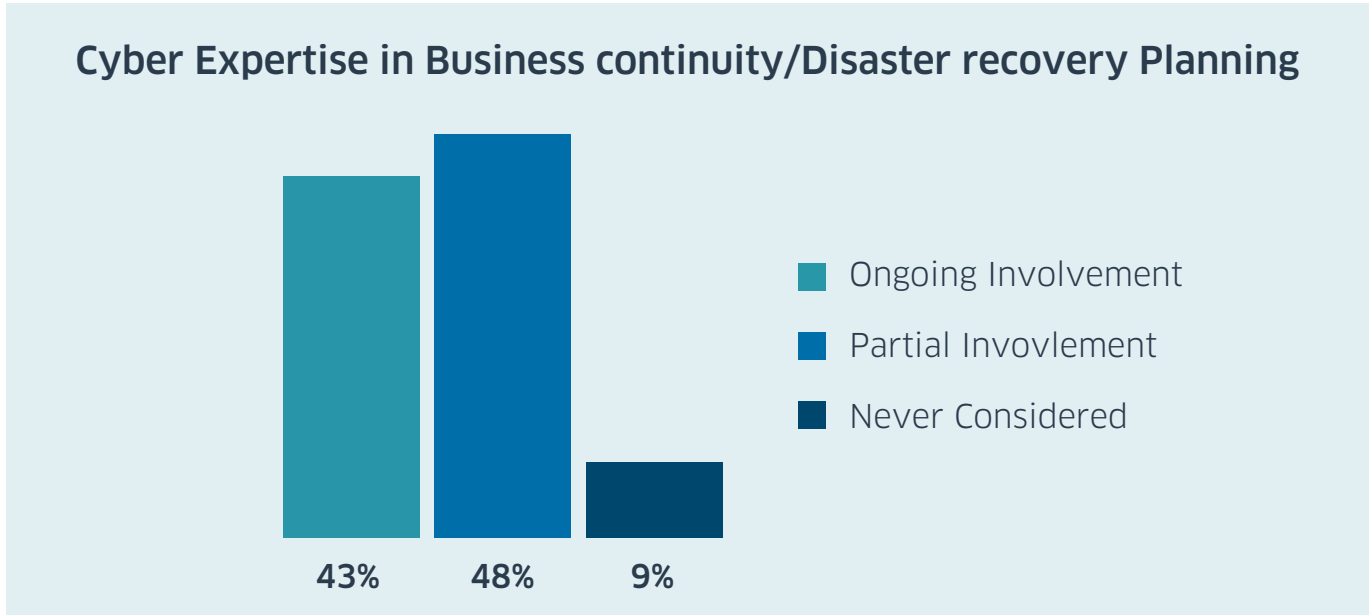
Preparedness is foundational to cyber resilience. SC3 recommends that public sector organisations invest in incident response planning, business continuity planning, staff training, and access to specialist incident response capability. Evidence suggests that organisations that have made these prioritisations in preparing for incidents recover faster and experience less impact than those that have not. The CRA provides detailed evidence of preparedness across the sector.

2.2.1. Preparedness in Numbers

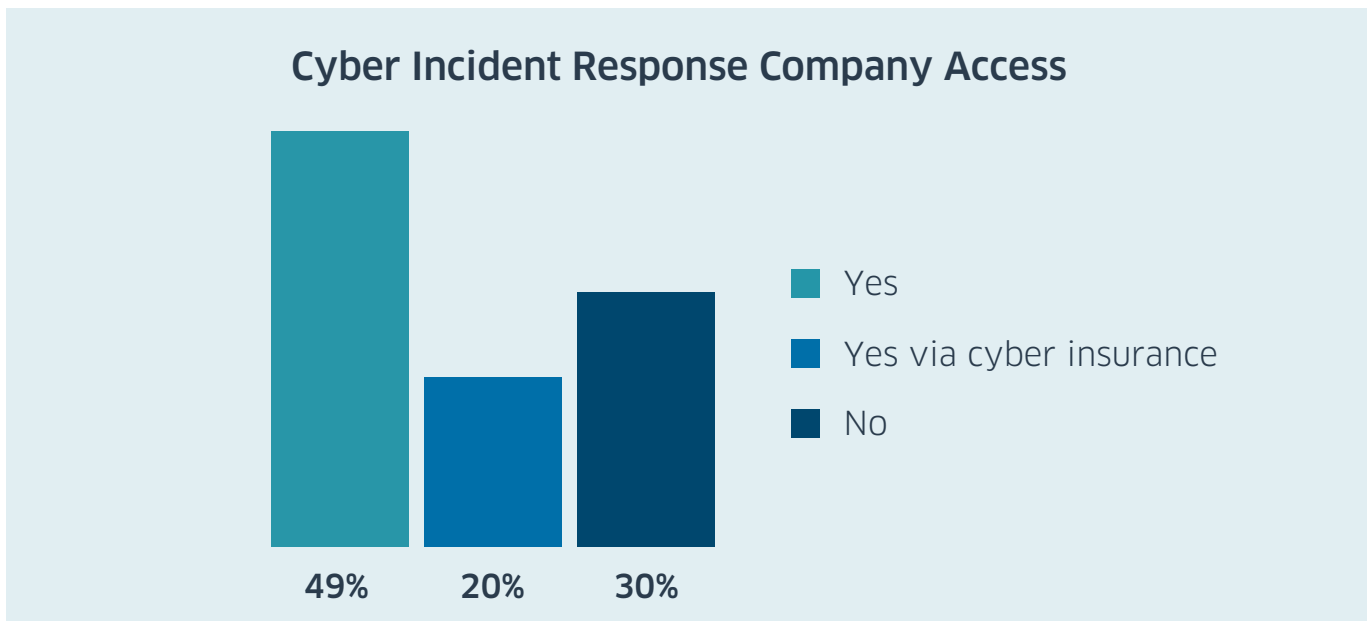
Most organisations surveyed reported having incident response plans in place.



This represents a relatively mature baseline. However, the finding that nearly one in five organisations have acknowledged gaps in their plans is significant. Complete loss scenarios where an organisation loses access to core digital systems for an extended period are increasingly realistic and demand specific planning. These scenarios are a significant burden to any sector, and in the public sector the significance cannot be understated. Business continuity and disaster recovery planning show similar patterns.



A critical component of incident preparedness is access to specialist cyber incident response (CIR) and forensic capability.



When organisations without a CIR provider experience a major incident, they must rapidly identify and engage external providers, a process that consumes valuable time and may leave them without guidance during the critical early hours of an incident.

SC3 publishes several templates for incident response and playbooks for specific incidents.⁵ These documents are designed to help organisation in the sector begin to plan for a cyber incident. They provide best practice advice and guidance, and prove as a starting point for a comprehensive and detailed plan. The sector’s engagement with SC3’s resources is evident in website download statistics. The Generic Cyber Incident Response Plan has been downloaded 386 times, the Public Sector Incident Response Plan 255 times, and sector-specific playbooks (for phishing, ransomware, malware, supply chain, denial of service, and data loss) have collectively been downloaded over 1,100 times. These numbers suggest that many organisations are downloading structured guidance, though downloading and implementing are distinct activities. It also suggests that the documents published by SC3 are received by a wider audience than just the public sector, serving the wider resilience of the private and third sectors.

2.3. Incident Response

2.3.1 The Incident Coordination and Response Workstream

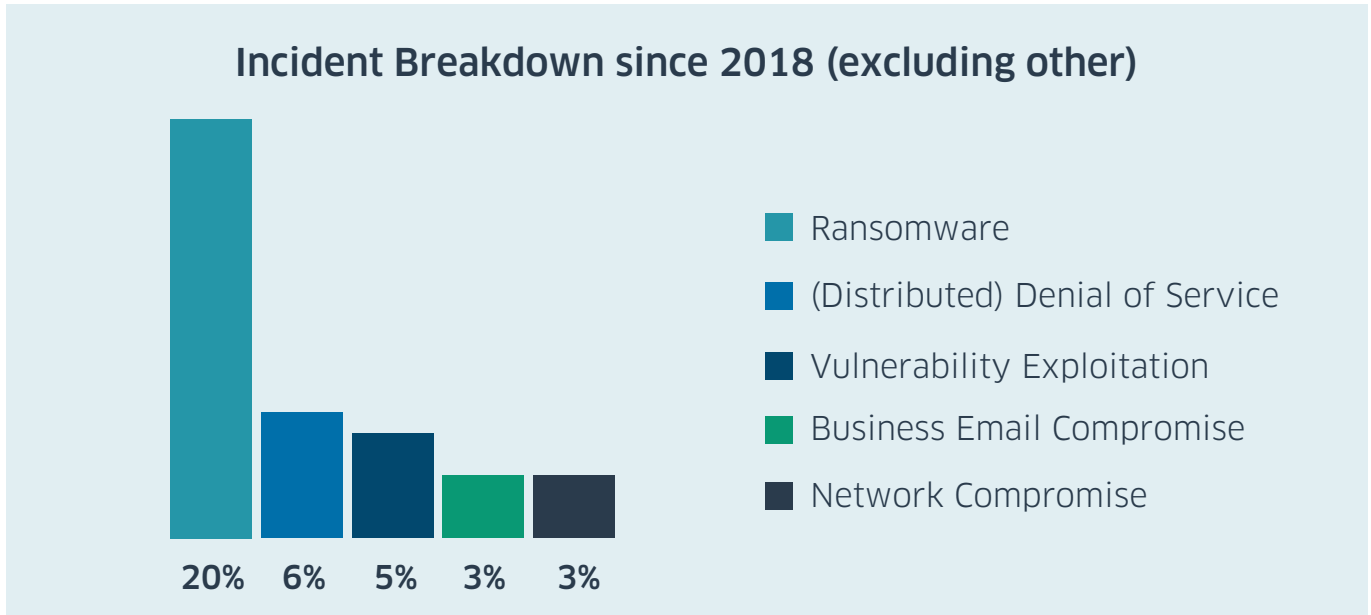
The SC3 Incident Response Workstream focuses on delivering rapid and consistent coordination across multiple agencies during significant or national-level cyber incidents. Its core purpose is to support affected organisations as they manage and recover from cyber events, while ensuring that essential information is communicated to stakeholders when required.

2.3.2 Incidents in Numbers

Between 2018 and early 2026, 183 incidents have been reported to SC3. A breakdown of recent incidents can be seen at the table below.

Year	Major	Minor	Total
2023	5	32	37
2024	4	32	36
2025	5	34	39

SC3 defines a major incident as one which requires a multi-agency response, beyond a routine situational awareness coordination. The balance of severity has been similarly steady, with major incidents representing roughly 12-14% of the annual total. Whilst many incidents do not reach the threshold of significance where national response arrangements led by the UK Government’s National Cyber Security Centre would be required, minor incidents still impose operational disruption and consume resources that smaller organisations do not have readily available.



Of the threats seen, ransomware is the most prevalent, accounting for 37 incidents. This aligns with the NCSC’s 2025 Annual Review, which identifies ransomware as the most pressing cyber threat to the UK. The NCSC reports that over 6,500 organisations globally were published on dark web leak sites in the year to August 2025, with the UK the fourth most targeted country. The emergence of ransomware-as-a-service platforms and malware-as-a-service marketplaces has lowered the technical barriers to entry, making this threat accessible to a widening pool of threat actors.

For comparative context, the NCSC’s 2025 Annual Review reports that its incident management team handled 429 incidents requiring direct support in the year to August 2025, from 1,727 tips received. Of these, 204 were classified as nationally significant which amounts to a 130% increase on the previous year’s 89, and 18 were classified as highly significant, a 50% increase.

The UK now faces an average of four nationally significant cyber-attacks per week. At UK level, the proportion of incidents classified as nationally significant has more than doubled in a single year, rising from 21% to 48% of the NCSC’s caseload. By contrast, SC3’s proportion of major incidents has remained stable at approximately 13% across 2023, 2024, and 2025, noting SC3’s specific remit of the public sector in Scotland.

3. Exercising

The cyber exercising workstream is one of the core pillars of the SC3. This workstream's primary objective is to enhance the cyber resilience of Scotland's public sector by ensuring organisations develop, maintain, and routinely test practical incident response capabilities.

Through simulated high-pressure cyber scenarios across technical, operational, and strategic levels, the workstream enables organisations to:

- Identify vulnerabilities and gaps within existing incident response processes.
- Test the effectiveness of their response plans in a safe, controlled environment.
- Strengthen operational coordination and decision-making.
- Improve technical incident handling and strategic crisis management.

The cyber exercising workstream aims to support public sector bodies toward a state of practically tested cyber resilience, ensuring they are able to effectively identify, respond to, and recover from cyber incidents through the following:

- Strengthening preparedness by:
 - Encouraging public sector organisations to prepare for the most common cyber attack scenarios.
 - Facilitating testing and improvement of Cyber Incident Response Plans (CIRPs) and playbooks.
 - Building sector-wide capability by developing a cadre of trained cyber exercising practitioners across the Scottish public sector to enhance resilience and increase exercising activity.
- Ensuring robust response processes such that:
 - All organisations have current, well-tested response plans.
 - National-level incident response processes are coordinated, robust, and effective.

3.1. Exercising in Numbers

In the past 12 months, **64%** of Scottish public sector organisations have reported they have carried out cyber exercising to test their cyber resilience arrangements. Whilst it is encouraging to see the uptake in exercising, there is still a significant number of public sector organisations that are not currently realising the benefits of cyber exercising. **58%** of organisations have reported undertaken tabletop exercising in the last year and **23%** of organisations reported having undertaken live play exercises.

A variety of tools and approaches have been utilised to deliver exercises across the sector including SC3 facilitated sessions, third party and Cyber Incident Response specialist facilitated exercises, as well as internal exercises using NCSC’s Exercise in a Box resources and the TTX Gym online cyber exercising tool among others. The following table shows the most common cyber exercising scenarios used across the Scottish public sector in the last year broken down by type of exercise:

Scenario explored in exercise	Tabletop exercises	Live play exercises
Ransomware attack	79	21
Data leak	38	10
Third party compromise	27	9
Supply chain	29	5
Managing a vulnerability disclosure	14	6
Other	35	14

Over the past few years, the SC3 Exercising Workstream has directly supported or facilitated 19 cyber exercises across the Scottish public sector. The figures in the table below illustrate the uptake of the cyber exercising support offer from SC3. Most of these exercises tested both the strategic and operational readiness of the organisations taking part in the exercise.

Sector	2025	2024
Central Government	7	0
Health	0	1
Local authority	3	7
Multi sector	1	0
Total	11	8

3.2. Exercising Themes

Common themes continue to emerge across the public sector and feedback gathered from organisations engaging in cyber exercising activities highlights strong support for continued and expanded exercising.

1. Exercises Build Engagement and Confidence

- Initial scepticism is common, but attitudes shift positively once exercises conclude and lessons are shared.
- Participants value the confidence, competence, and decision-making insights gained from TTXs.
- Exercises also function as effective team-building activities.

2. Localised Scenarios Are More Effective

- Staff respond better to bespoke, locally relevant scenarios than generic materials.
- Highlights the need for configurable scenario templates tailored to organisational contexts.

3. Resource Constraints Limit Follow-Through

- Exercises routinely surface long lists of lessons, but many organisations lack capacity to implement them.
- Some organisations have not yet exercised due to staffing/resource shortages.
- Indicates value in shared SC3 support, templates, and potentially facilitation services.

4. Looking Ahead

4.1. Themes & Lessons

The SCAR demonstrates a clear set of cross-cutting themes that should inform strategic decision-making across Scotland's public sector.

Cyber risk is systemic. It affects organisations across all sectors, all sizes, and all levels of digital maturity. It cannot be solved by individual organisations acting alone. This is the fundamental rationale for collaboration, information sharing, and coordinated response. The sector requires shared threat intelligence, coordinated vulnerability disclosure, and forums for collective learning. This is precisely the role that SC3 is designed to fulfil, and collaboration across the public sector is essential for the continued improvement of cyber resilience.

Leadership and governance are the primary outcome-drivers. Technical controls such as firewalls, endpoint protection and intrusion detection systems are necessary but not sufficient. The ability of organisations to detect incidents quickly, make rapid decisions about response and recovery, communicate effectively, and learn from the experience depends primarily on governance and leadership capability. This places responsibility squarely on boards and senior leaders, not on IT departments. Governance frameworks for cyber risk, incident response planning that assigns clear decision-making authority, and board-level awareness and oversight are the most critical investments organisations can make.

Business continuity plans for digital services need improvement. Current business continuity plans, developed over time to handle system failures, financial disruptions, and supply chain interruptions do not adequately address the scenario of sustained digital infrastructure failure over a period of days and weeks, not hours. The sector requires business continuity and disaster recovery plans explicitly scoped for cyber scenarios, tested through exercises, and regularly refreshed. This is particularly critical for organisations that have not experienced a cyber incident as the assumptions embedded in their plans are untested and likely to be unrealistic.

Communications is not a secondary concern, it determines outcomes. The reputational consequences of how an incident is communicated can exceed the technical consequences. Organisations require dedicated communications plans for cyber incidents, pre-established governance and decision-making authority, and trained communicators. Communications planning should be integrated into incident response planning, not treated as an afterthought. Alternative communication strategies are equally important, and how an organisation communicates when primary systems are down. When an organisation loses the ability to communicate internally (because email is compromised or unavailable), or cannot communicate externally (because its website is down or its public comms channels are controlled by an attacker), the incident rapidly becomes a crisis of confidence. Staff and colleagues do not know what is happening. Citizens and clients do not receive information. Media narratives develop without counter-narrative.

Incident response capacity is a sector-wide concern. Whilst most organisations have incident response plans, access to specialist incident response support is not universal. This is a gap that requires active management, potentially through closer integration with commercial CIR providers or expanded public sector capability. The pandemic revealed the vulnerability of distributed incident response; cyber incident response would likely overwhelm existing capacity if multiple large organisations were compromised simultaneously.

Data theft and extortion require strategic thinking, not just technical response. Early ransomware typically encrypted data and demanded ransom for decryption. Modern ransomware increasingly combines encryption with data exfiltration, or even bypassing the encryption process altogether, threatening to publish stolen data if the organisation refuses to pay. Whilst there has been investment into ransomware protection, evidence now suggests threat actors are focusing on data exfiltration as a primary source of extortion.

Technical controls need to be put in place. Organisations should define and routinely monitor baselines for normal network and system activity. Staff must be provided with clear guidance to help them recognise indicators of suspicious behaviour. Out-of-hours monitoring and escalation arrangements need to be robust, ensuring that responsibility does not fall on a single individual and that there are no single points of failure. Backups must be immutable, regularly tested, and resilient against ransomware. To support effective recovery sequencing, organisations should have a thorough understanding of their system dependencies, including those hosted on-premises, in the cloud, or delivered by third-party suppliers. Disaster recovery strategies should account for scenarios involving partial system loss, full system failure, and long-term service degradation.

Supply chain risk is critical. Organisations have limited visibility into their supply chain and do not regularly assess the cyber risk posed by suppliers. Through-life assurance is limited, and as supply chain attacks become more common, this represents a significant vulnerability. The sector requires standardised approaches to supplier assurance, shared understanding of acceptable cyber practices among suppliers, and coordinated approaches to managing supply chain risk.

Regular exercising is a must. Exercises should be conducted regularly and designed to be as realistic as possible, involving business units, executive leadership, and technical teams. These exercises need to incorporate challenging scenarios such as prolonged outages, the loss of identity systems, loss of email services, and extortion-based attacks to ensure organisations are prepared for the types of disruption that are increasingly common. Crucially, any lessons identified during these exercises must lead to lessons implemented. This requires structured follow-up mechanisms that ensure actions are tracked, completed, and embedded into organisational practice, rather than remaining as observations without meaningful change.

Education Networks in Local Authorities represent a specific area of concern. Incident data reveals that education networks operated by local authorities lack adequate security measures compared to their corporate network counterparts. These education networks often handle significant volumes of data relating to children and young people. The disparity in security posture between corporate and education networks within the same organisation suggests that education networks are not subject to the same governance, investment, and monitoring standards as the primary corporate infrastructure. Given the sensitivity of the data they hold and the potential for them to be exploited as an entry point to the wider network, this gap requires urgent attention.

Lessons must be identified and shared faster. The current pace at which lessons are captured from incidents and disseminated across the sector is not sufficient. The sector requires structured mechanisms for rapid lesson capture, anonymisation where necessary, and timely dissemination. SC3 has a central role to play in accelerating this process, but organisations must also commit to contributing their own lessons openly and promptly.

The themes and lessons identified in this report are not theoretical. They are grounded in the real experience of Scottish public sector organisations that have faced significant cyber incidents. Two cases of organisations who have published reports on their incidents illustrate the recurring nature of these challenges and, critically, the sector's difficulty in absorbing and acting on lessons at pace.

In December 2020, the Scottish Environment Protection Agency (SEPA) was targeted in a ransomware attack by the Conti criminal group. The attack occurred on Christmas Eve, when staffing was at its lowest, and resulted in the encryption of critical systems and the theft and subsequent publication of approximately 1.2 gigabytes of data.

SEPA's recovery was extensive; the organisation took the strategic decision to rebuild its digital infrastructure from new rather than attempt to restore compromised legacy systems. A formal lessons learned review was published in late 2021, identifying 44 discrete lessons across areas including incident response frameworks, business continuity, backup integrity, network segmentation, communications, staff welfare, and multi-agency coordination. The review was transparent and widely shared across the public sector, and the wider public in their report.⁶

In November 2023, nearly three years after the SEPA attack, Comhairle nan Eilean Siar (Western Isles Council) was struck by a ransomware attack that caused severe disruption to council services. The attack encrypted on-premise systems, rendering many core services unavailable. Recovery extended over a year, with some systems still not fully restored twelve months after the incident. The financial impact exceeded £1 million in one-off and ongoing costs. Five IT vacancies at the time of the attack compounded the challenge, and the strain on staff was described as overwhelming all of which was detailed in their own published report.⁷

The lessons identified from the Western Isles incident are strikingly similar to those identified by SEPA three years earlier. Both organisations found that business continuity plans were inadequate for enterprise-scale digital failure. SEPA discovered that emergency management procedures stored on compromised systems were inaccessible when needed most; the Western Isles found that corporate business continuity plans were used inconsistently across departments and were not scoped for a cyber scenario of this magnitude.

Both organisations identified the critical importance of leadership and command structures in driving recovery. Both highlighted communications resilience as essential, SEPA was praised for its transparent external communication, whilst the Western Isles review noted that internal communications were sporadic and staff felt uninformed. Both reported severe workforce strain, with small teams carrying unsustainable workloads over extended recovery periods. Both identified gaps in detection and monitoring capability, with the Information Commissioner's Office specifically highlighting to the Western Isles the need for a Security Information and Event Management (SIEM) system and enhanced endpoint monitoring, capabilities that SEPA had already identified as priorities in its own review.

One notable finding from the Western Isles review was that the council's schools network, which operated on a separate infrastructure, was largely unaffected by the attack. This physical separation likely prevented the ransomware from spreading to education systems. However, as noted elsewhere in this report, education networks in many local authorities lack the same level of security investment as corporate networks. The Western Isles case demonstrates both the protective value of network segmentation and the risk that, in other authorities where such separation does not exist, education networks could serve as either an entry point or a casualty of a wider attack.

Many of the lessons identified from both incidents are demonstrated in this report, showing that the lessons are not unique to victim organisations, but indeed the whole sector. In publishing the SCAR, SC3's hopes are that these core issues are identified and addressed within each public sector organisation.

4.2. Conclusion

Scotland faces a cyber security challenge that is systemic, persistent, and evolving. Cyber attacks affect organisations across all sections of the public sector. They impose operational, financial, and reputational costs. They undermine public confidence and can disrupt essential services. Yet the evidence presented in this report demonstrates that resilience is achievable. Organisations that have invested in governance, planning, exercising, and capability have recovered quickly from incidents and have maintained public confidence. The sector collectively possesses examples of good practice, and the knowledge of what works.

The challenge is to spread this good practice more widely and to address the gaps that remain. 30% of organisations lack formalised incident response support. Nearly half have not fully integrated cyber risk into business continuity planning. Many organisations lack dedicated cyber incident communications plans. Lessons from incidents are not being identified and shared across the sector quickly enough to prevent recurrence. These gaps are addressable through focused effort and investment. The fact that some organisations have solved these problems demonstrates that the solutions are available; what is required is the will to implement them across the sector.

SC3 is Scotland's focal point for coordinating this work. Through its standards and insights, threat intelligence, vulnerability coordination, incident management, and exercising workstreams, SC3 facilitates the sharing of learning, the development of common approaches, and the building of relationships across the sector that enable rapid response when incidents occur. This report is published to support that work, to inform senior leaders about the cyber risk facing Scotland's public sector, and to highlight the actions required to reduce that risk.

The coming year will be critical. The sector should treat the recommendations in this report as a starting point for a conversation about cyber resilience at board level, at leadership level, and across the sector. Investment in governance, planning, and exercising will pay dividends in the form of faster incident response, less operational impact, and greater public confidence.

The Strategic Framework for a Cyber Resilient Scotland sets out the vision that Scotland thrives by being a digitally secure and resilient nation. Whilst there is work to be done, collaboration is embedded across the public sector, and with SC3 as a focal point of coordination, this vision is within reach.

5. References

- 1 [NCSC Annual Review 2025 | National Cyber Security Centre - NCSC.GOV.UK](#)
- 2 [Cyber security breaches survey 2025 - GOV.UK](#)
- 3 [Cyber Resilient Scotland 2025 to 2030: strategic framework - gov.scot](#)
- 4 [Scottish Cyber Coordination Centre: SC3 strategic plan 2024 to 2027 - gov.scot](#)
- 5 [Cyber incident response toolkit - gov.scot](#)
- 6 [SEPA's response and recovery from a major cyber-attack](#)
- 7 [Cyber Attack Response and Lessons Learnt](#)



© Crown copyright 2026

OGL

This publication is licensed under the terms of the Open Government Licence v3.0 except where otherwise stated. To view this licence, visit nationalarchives.gov.uk/doc/open-government-licence/version/3 or write to the Information Policy Team, The National Archives, Kew, London TW9 4DU, or email: psi@nationalarchives.gsi.gov.uk.

Where we have identified any third party copyright information you will need to obtain permission from the copyright holders concerned.

This publication is available at www.gov.scot

Any enquiries regarding this publication should be sent to us at

The Scottish Government
St Andrew's House
Edinburgh
EH1 3DG

ISBN: 978-1-80775-056-5 (web only)

Published by The Scottish Government, March 2026

Produced for The Scottish Government by APS Group Scotland, 21 Tennant Street, Edinburgh EH6 5NA
PPDAS1724786 (03/26)

W W W . g o v . s c o t