Taking Stock

A report on progress towards a cyber resilient Scotland

October 2023

Scottish Government
Riaghaltas na h-Alba

Contents

Section 1: Forewords

The Strategic Framework for a Cyber Resilient Scotland was published in February 2021, during a period of significant disruption. The global pandemic accelerated Scotland's transition to a digital economy and society, transforming the way we work, learn, shop, socialise and use public services. The possibilities of digital technologies will continue to shape how we live, and how the public and private sectors operate. Interconnectivity has great benefits, but it can also make us, our communities, our businesses and institutions vulnerable.

We continue to see an increase in cyber risk to our organisations, businesses and personal security. Threats such as ransomware, online fraud, data theft and disruptive attacks are growing in sophistication and frequency. Hostile state actors and cyber criminals target our critical national infrastructure, our public services, our businesses, and scientific research. The borderless nature of cyberspace increases the risk and complicates our response. The Scottish Government takes the growing risk seriously, and works closely with the UK Government, the National Cyber Security Centre (NCSC), Police Scotland and many others, to put in place appropriate mitigations.

The Scottish Government's priority has been on helping to build the public sector's capacity to withstand and manage cyber risk, and I am reassured that we are beginning to see improvements. We have also been endeavouring to protect individuals, especially the most vulnerable in our communities, and to equip them to stay safer and more secure online. At the same time, we have been working to grow a more diverse cyber security skills pipeline to meet the skills gap that Scotland shares with the rest of the world, and we are gaining international recognition for our advances in this area.

Now that the worst of the pandemic is behind us, it is time to take stock of our work to date. I am pleased to present this report, which recognises what has been achieved in Scotland, but which also identifies the risks, opportunities and gaps in our current approach, as well as setting out our future priorities.

I want to thank all the partners involved in getting us to where we are today, and I look forward to continuing our work alongside all stakeholders to build a more secure, resilient and prosperous Scotland.

Angela Constance, MSP
Cabinet Secretary for Justice and Home Affairs

The Strategic Framework sets out the approach Scotland is taking to create a digitally secure and resilient nation and is deliberately broad reflecting Scotland's ambitions.

We recognise that we live in turbulent times and as we embrace new technology and rely on interconnected technology – both for public services and for our own personal use – the attack surface is changing and expanding, offering threat actors such as criminals and hostile states an increased opportunity to attack us for disruption or monetary gain. It is vital that we are prepared as a nation to deal with the threat and to be resilient to it.

This report shows how far we have come since the Framework was launched; but this is not the time to be complacent, rather, we need to be ambitious. Our adversaries are better funded and better resourced than we are - they are agile and can embrace technology and tools much quicker and they can change attack direction as new opportunities arise. If we do not continue to invest in being cyber resilience, we will fall behind and this will adversely impact our citizens and our businesses.

We recognise this is not something which can be done by government alone, nor indeed Scotland alone. We rely on our partnerships across the UK nations and build upon what has already been achieved.

There are three key areas where I feel we need a step change in delivery:
Skills – the report highlights progress, which is really encouraging, but the pace of change and the numbers delivered are insufficient for the vacancies across the public and private sectors. Employers have highlighted that candidates lack the skills for vacancies which they cannot fill. We must do more to ensure that Scotland gives students from all backgrounds the opportunity not only to learn cyber security, but to know about the substantial number of cyber security career opportunities open to them. Also, we need to take the opportunity to upskill and retrain specific groups in cyber security, such as our veterans who may be able to plug the vacancy gaps in cyber.

When considering cyber careers in public sector bodies such as Police Scotland and local authorities, the public sector cannot compete with private sector salaries. We need to develop ways to share resources across sectors which enable the public sector to mature and protect our citizens. And we need innovative technology to deal with the volume of data allowing skilled resource to make quicker evidence-based decisions. This is the second step change I would like to see happen.

We rely on our partnerships and collaboration across the UK, our work with the public and private sectors to raise awareness of the cyber threat and our work to deliver skills for old and young. Our investment to help small businesses, part of the lifeblood of our economy, improve their cyber defence is key to economic growth. I am also enthused by Scottish Ministers' decision to establish the Scottish Cyber Coordination Centre (SC3). The successful delivery of a fully operational SC3 is the third priority which will require sustained investment if we are to truly improve our abilities to manage and response to cyber incidents.

This is a whole team game, and as Chair of the National Resilience Advisory Board, I can confirm that my Board is committed to working with Ministers, officials and our strategic partners to deliver against each of the programmes of work to build a safe, secure and resilient future for Scotland.

Maggie Titmuss, MBE
Chair of the National Cyber Resilience Advisory Board

Section 2: Executive Summary

Introduction and context

Since 2015, steps have been taken to defend Scotland against cyber threats, and to further develop Scotland's cyber security posture.

Scotland's first strategy, Safe, Secure and Prosperous was published in November 2015 and laid the groundwork for Scotland to become more cyber resilient. The Scottish Government (SG) reflected on this strategy in its progress report Firm Foundations, published in November 2020.

In February 2021, SG published its second cyber resilience strategy The Strategic Framework for a Cyber Resilient Scotland (the Strategy). The Strategy sets out the vision of Scotland thriving as a digitally resilient, safe and secure nation. It outlines four outcomes in response to evolving threats, emerging opportunities, and the need for collaborative action.

The Strategy has four Action Plans (Public Sector, Private Sector, Third Sector, and Learning and Skills) which set out the priorities for both government and partners. As the Strategy was designed to be responsive to changing needs, priorities can be added or adapted, so that its focus can shift according to the current cyber threat and political, economic and societal pressures.

The Strategy is aligned to the UK Cyber Strategy, which outlines pillars for the four nations to improve cyber security, with Scotland's primary contribution focused on the Cyber Ecosystem and Cyber Resilience pillars.

This report, Taking Stock, is a review of the impact of our strategic activities since 2015, and sets out our priorities for the future.

The scale of the threat

The global landscape has changed substantially since the Strategy was published in 2021. The COVID-19 pandemic forced the people of Scotland, businesses and organisations to work, learn, socialise and trade online. While Scotland's online participation has many benefits, it also exposes us to an evolving threat landscape.

There has been a rise in the number and sophistication of cyber threats. Threat actors take advantage of our dependency on Internet-connected technologies in order for them to conduct malicious activities. Policing is also facing growing challenges to keep pace with the cyber criminals. Investigating, mitigating and countering cyber crime can be complex and resource-intensive, made more difficult by the borderless nature of cyber crime.

Cyber security workforce shortages continue to be a pressing challenge for governments, businesses and organisations, both in Scotland and internationally. Global tensions are ever present, and we must be alert to protecting our population, our national interests and our prosperity, particularly during periods of uncertainty.

Progress and priorities going forward

Effective leadership and partnership

Key achievements:

- The Scottish Government has demonstrated leadership by engendering collaboration and coordination of cyber resilience activity between stakeholders and partners.
- Partnerships across sectors in Scotland, alongside the UK Government and the National Cyber Security Centre (NCSC), have enhanced Scotland's ability to protect ourselves from cyber crime and respond more effectively to emerging threats.
- The establishment of two flagship entities: the CyberScotland Partnership (CSP) and the Scottish Cyber Coordination Centre (SC3).
- The CSP (a collaboration of national agencies and representative bodies) is helping to coordinate and augment cyber messaging across Scotland and is growing in strength with structured communications and events planning. The CSP is a single source of information and guidance via the CyberScotland portal and bulletins.
- The SC3 is in its infancy but is positioned to become the central coordination function for improved intelligence sharing, early warning and incident coordination in Scotland with strong connections into the NCSC and the UK Government's Cyber Coordination Centre, which is also in development.
- The National Cyber Resilience Advisory Board continues to provide strategic advice and challenge to Scottish Ministers.

Looking ahead - key priorities:

- The Scottish Government, in collaboration with its partners across sectors, UK and beyond, will continue to take a leadership role to advance cyber resilience in Scotland.
- Partnership-working will be central to achieving our ambitions. National stakeholders will collaborate through the pro-active CyberScotland Partnership (CSP).
- The SC3 will be appropriately led, governed and resourced to be able to more effectively share intelligence, respond to evolving threats and help defend critical systems.

An innovative and joined-up cyber ecosystem

Key achievements:

- The Scottish Government's leadership has helped to build Scotland's cyber security sector, but we continue to face challenges in meeting the growing demands for cyber talent in Scotland.
- Increased awareness of cyber threats among the general population with people's cyber hygiene is broadly improving.
- The CSP is committed to building cyber resilience with its audiences, communities and networks.
- The skills pipeline is strengthening, with an increase in the offer of cyber security qualifications at all educational levels and in vocational training.
- General cyber resilience learning is now embedded in the 3-18 school curriculum with early evidence of effective learning and teaching taking place in an increasing number of schools.
- Many youth engagement organisations are running successful tailored campaigns from which we are beginning to see increased awareness of online risks amongst our younger population.
- Specific support and guidance is reaching Scotland's SMEs.
- Growth in Scotland's cyber security products and services industry is at a rate similar to that across the rest of the UK.
- Targeted work with older people and people with additional language and other barriers is beginning to help to build cyber confidence.

Looking ahead - key priorities:

- Continue to increase the reach and uptake of advice and guidance amongst the general public, businesses and organisations, through a range of means and measures.
- Focus on improving online protective behaviours of the general public in line with Cyber Aware messaging, with additional effort on raising the cyber resilience of young people and older people, and to reach people who need information to be presented in alternative or accessible formats.
- Encourage the reporting of cyber incidents to Police Scotland.
- Continue to increase cyber security skills and grow the talent pipeline to meet the increasing demand for cyber security jobs, and to enhance innovation and research.
- Increase diversity within the cyber security workforce.
- Supporting the roll out of professional cyber security standards in cyber security roles.

- Support the growth of the Scottish cyber security products and services industry.
- Promote the adoption of relevant cyber security standards of Managed IT Service Providers and encourage them to be clear on the extent of the cyber security support they offer.
- Encourage and support private and third sector organisations to increase their cyber resilience maturity through improved understanding of cyber risks and threat/intelligence sharing, adopting cyber resilience best practice measures including incident response planning and exercising.
- Build momentum in the adoption of Cyber Essentials in Scotland.
- Embed cyber risk into organisations' board and senior management structures.

A maturing public sector

Key achievements:

- Scotland's public sector organisations are becoming better prepared against the cyber threat, although there is much more to do.
- Increasing numbers of public bodies are reporting that their workforces, senior management, and board members are undertaking cyber security training. While most organisations now have an incident response plan in place, there is a need for them to regularly exercise and test their plans.
- Scotland's national cyber incident response arrangements are in place and are regularly exercised.

Looking ahead – key priorities:

- The public sector continues to build its cyber capability, particularly around incident response, exercising, cyber awareness training for board members, threat/intelligence sharing and independent cyber assurance.
- Focus more national support on those public bodies where cyber incidents could be catastrophic.
- Maintain and reinforce our national cyber incident response and intelligence sharing arrangements through the evolution of the Scottish Cyber Coordination Centre.
- Support cyber security professional development across the public sector.
- Increase general cyber resilience awareness amongst the public sector workforce.

Conclusion

Scotland continues to be confronted by the challenges of an increasingly complex cyber threat environment. Cyber crime, online fraud and ransomware are increasing in volume and complexity. The evolution and use of advanced technologies such as Artificial Intelligence will only add to these challenges.

Scotland's aim for security and prosperity in the digital age relies on leadership as well as partnership with local government and the public, private, and third sectors. The next iteration of the public, private and third sectors and learning and skills actions plans, due to be published in the autumn of 2023, will provide direction for us to achieve this.

Scotland must remain agile to the ever-evolving cyber threat. The Scottish Government will continue to protect against threats that target Scotland, working closely with the UK Government and the NCSC as well as it vital partners.

Section 3: Introduction

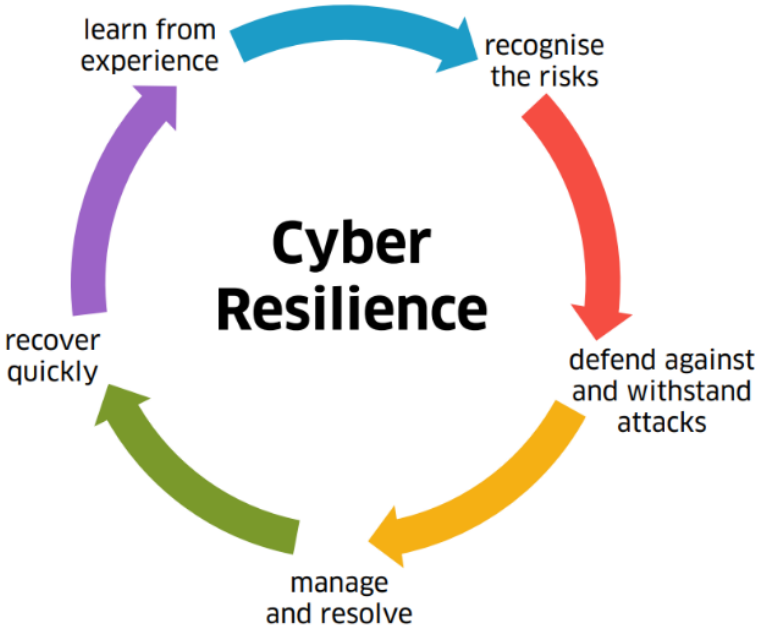
This report considers how Scotland is progressing in its cyber resilience maturity. . It details how the implementation of the Scottish Government's (SG) cyber resilience policy has contributed to improving the cyber resilience of Scotland's citizens, organisations and businesses.

The findings in this report will help inform the direction of SG's priorities going forward as we continue in our collective work to realise our vision of Scotland thriving as a digitally safe and secure nation.

Cyber resilience

Cyber resilience underpins Scotland's ambitions for economic growth, resilient public services, digital inclusion, crime prevention, and for building safer and more resilient communities.

Cyber resilience goes beyond simply making technologies and systems secure. It also incorporates an understanding of the cyber threat, the acquisition of skills to become prepared to withstand and manage threats, as well as the ability to recover quickly and learn from cyber incidents.



Scale of the cyber threat

The financial costs of cyber crime are difficult to calculate, as they can include the financial loss to victims, reputational damage and the costs of responding to and recovering from an incident. Cyber crime is estimated to cost the UK billions of pounds each year[1].

In 2022-23, Police Scotland recorded 14,890 cyber crimes.[2] This number has been broadly stable over the past 3 years but represents a significant increase from the estimated 7,710 cyber crimes recorded in 2019-20. Part of the increase may be due to the COVID-19 pandemic, increased digital adoption as well as wider public awareness of how to report cyber crime. In 2022/23, an estimated 5% of all recorded crime was cyber crime and 51% of all fraud was cyber fraud. Cyber crime is underreported, so the actual numbers could be much higher.

[1] Home Office, Understanding the costs of cyber crime (2018)
[2] Scottish Government, Recorded Crime in Scotland, 2022-2023 (2023)

The compromise of the supply chain and ransomware are currently two of the biggest threats to organisations and businesses. Ransomware was classified as a tier 1 national security threat in 2023[3] and the UK was the third most impacted country (after the United States and Canada) in terms of the number of organisations that experienced a ransomware incident in 2022[4].

Although ransomware has evolved in both sophistication and complexity, and is a significant business disruptor, most incidents do not involve specific targeting. Instead, they are part of automated, opportunistic campaigns with cyber criminals taking interest only when they identify vulnerabilities in an organisation's defences.

In recent years, a business model has emerged known as Ransomware as a Service (RaaS). Ransomware operators create and sell ransomware to affiliates who launch the attacks. This reduces the barriers of entry to actors who wish to carry out ransomware attacks but lack the technical capability to develop the malware themselves.[5]

Scotland has been affected by several ransomware incidents in recent years, including those faced by the Scottish Environment Protection Agency (December 2020), Scottish Association for Mental Health (March 2022), the NHS supplier One Advanced (August 2022) and Royal Mail (January 2023).

One of the most prolific ransomware gangs, Conti (which claimed responsibility for the Scottish Environment Protection Agency (SEPA) cyber incident in December 2020) caused breaches in over 600 organisations worldwide since its emergence in late 2020. The growth in their payment requests, from an initial $118 thousand in 2020 to an average of $1.78 million during 2021, reflects their growing capacity and activity.[6]

The ransom is only part of the total cost to organisations. They may also lose intellectual property and data, experience reputational harm, and suffer costs associated with lost productivity as a result of having to restore and rebuild their systems and replace devices.

Supply chain attacks are another major threat to Scotland's organisations. Most organisations rely on suppliers to deliver products, systems and services. However, supply chains can be large and complex. Securing the supply chain can be difficult because vulnerabilities can be inherent or introduced and exploited at any point in the supply chain.

Threat to political stability and democracy

Threat actors continue to seek to destabilise democratic processes for political purposes through a number of means. These include disinformation campaigns,

[3] UK Government, Press release: UK cracks down on ransomware actors (2023)
[4] Palo Alto, Unit 42, Ransomware Threat Report 2022 (2022)
[5] Crowdstrike, Ransomware as a Service (RaaS) Explained (2023)
[6] Palo Alto, Unit 42, Ransomware Threat Report 2022 (2022)

disruption of online services and theft of sensitive information. The threat can become particularly heightened during election periods.

For example, in November 2022 the European Parliament's websites were disabled by a Distributed Denial of Service (DDoS) attack, just a few hours after the resolution expressing support for Ukraine was passed. In 2021, ransomware was used to elicit support for protesting farmers in India. In this case, the victims were told they could recover their encrypted data only after the farmers' political demands were met.

Government Ministers are advised not to use private email accounts to do government business; however, their private accounts are targeted as they are likely to be less secure than their corporate/official accounts. Gaining access to these private accounts can also make it easier for hackers to access official accounts and systems. As our electoral processes become progressively more digitised, there are increasing security considerations for those planning, and those running for, election. The Scottish Government and the NCSC continue to work closely with the Scottish Parliament to ensure that appropriate cyber mitigation measures are in place.

Scotland's Cyber Resilience Policy

National action to improve cyber resilience in Scotland was first formalised by Scottish Ministers in 2015 with the publication of Scotland's first cyber resilience strategy: Safe, secure and prosperous: a cyber resilience strategy for Scotland. It put in place many of the building blocks to strengthen Scotland's ability to prepare for, withstand and recover from cyber attacks.

November 2015

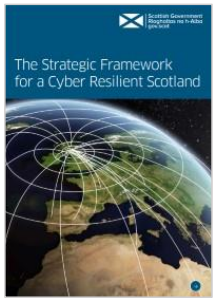
Safe, Secure and Prosperous: A Cyber Resilience Strategy

November 2020

Firm Foundations Progress Report

February 2021

The Strategic Framework for a Cyber Resilient Scotland



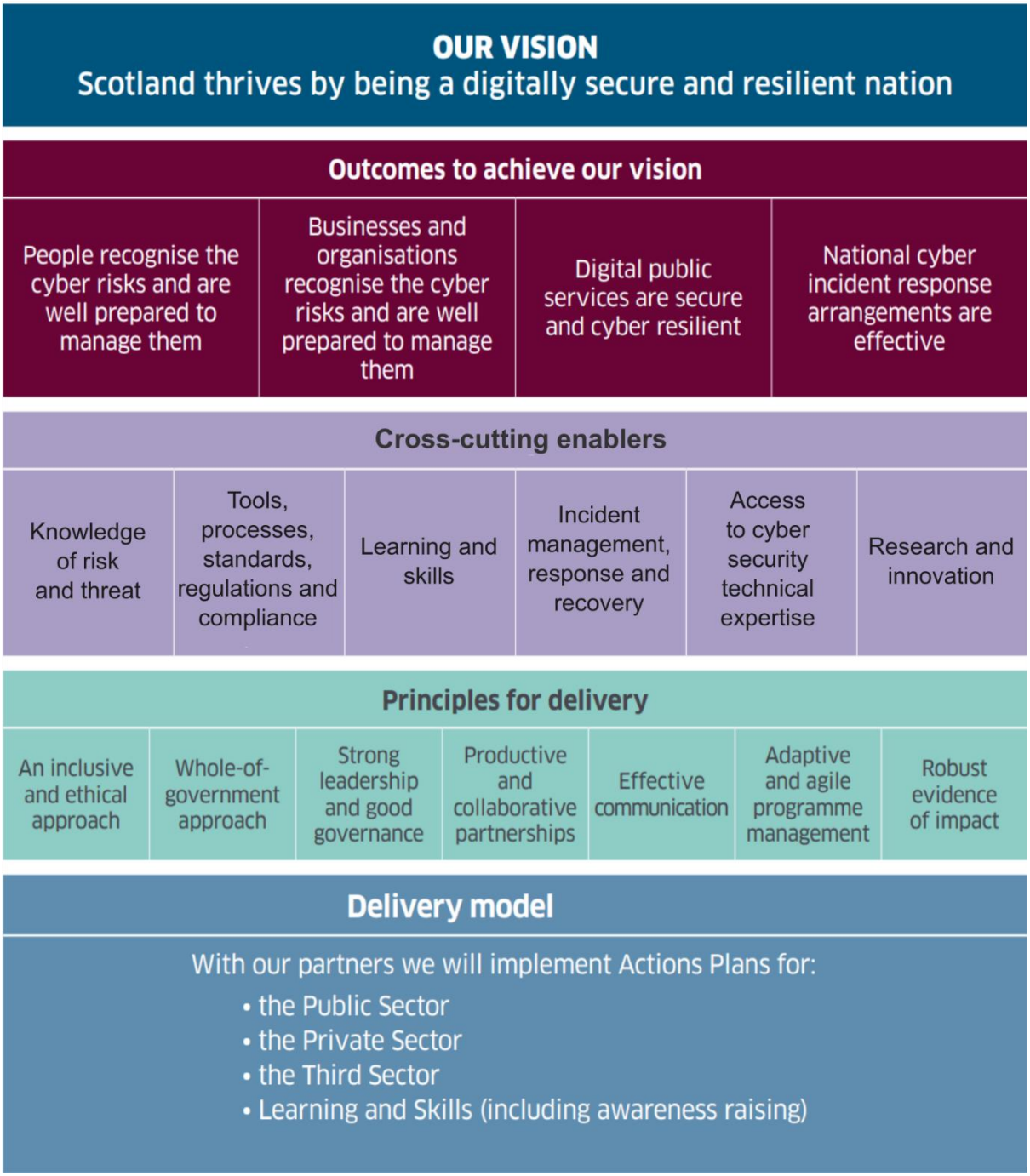
October 2023

A Cyber Resilient Scotland: Taking Stock

When Scotland's second strategy, The Strategic Framework for a Cyber Resilient Scotland was published in February 2021, Scotland faced many new and unexpected challenges including the severe disruption of the COVID-19 pandemic, the rapid shift to digital technologies and the Internet, and increased geo-political tensions.

Within this complex and ever-shifting landscape, cyber resilience clearly emerged as a critical enabler to ensure that people, businesses and organisations benefitted fully from digital and online services and solutions

Our strategic approach aligns closely with the objectives in The National Cyber Strategy, published by the UK Government in December 2021. It also aligns with the Scottish Government's Digital Strategy and Building Resilient Communities, and delivers on the National Performance Framework.



Improving cyber resilience through strong governance and partnership

Governance

The Scottish Government's Cyber Resilience Unit (SG CRU) is responsible for leading on the development, implementation and reporting on the impact of cyber resilience policy in Scotland. The National Cyber Resilience Advisory Board brings together leaders and influencers from across the private, public and third sectors to provide strategic advice, challenge and support to Scottish Ministers.

The SG CRU connects our work with that of the UK Government's Cyber Strategy, inputting evidence into the UK Government's cyber performance framework.

Partnership

The cyber threat to Scotland cannot be addressed by government alone. The SG CRU has led on forming a successful and pro-active partnership to drive forward cyber communication campaigns and deliver Cyber Scotland Week, reaching diverse audiences and communities across sectors in a coordinated and coherent way.

The CyberScotland Partnership (CSP) members include CENSIS, College Development Network, Cyber and Fraud Centre Scotland, Education Scotland, Highlands and Islands Enterprise, IASME Consortium, LEAD Scotland, NCSC, Police Scotland, ScotlandIS, Scottish Council of Voluntary Organisations (SCVO), Scottish Enterprise, Scottish Government, Scottish Social Services Council (SSSC), Skills Development Scotland (SDS), UK Cyber Security Council, YoungScot and YouthLink Scotland.

During CyberScotland Week 2023, 133 events took place across the country, raising awareness of the cyber threat, encouraging networking and promoting cyber security learning opportunities and careers.

Improving Scotland's ability to share intelligence and respond to incidents

In 2022, Scottish Government's Covid Recovery Strategy stated the need for a recognised, authoritative and collaborative central function to combat the accelerating cyber threat to Scotland.

The Scottish Cyber Coordination Centre (SC3) has been set up to pool expertise from partner organisations and centres of cyber security expertise (Police Scotland, NHS National Services Scotland, HEFESTIS, the Scottish Government, the Cyber and Fraud Centre Scotland, the Digital Office and the NCSC) to improve sharing of intelligence and response to risks. In its early stages, it will focus on intelligence collection and sharing, early warning notification and incident management coordination.

The Scottish Cyber Coordination Centre is a significant leap forward for Scotland and will raise our capabilities and capacity to tackle the threat, risk and harm that cyber incidents pose and cause. It is an integral part of our multiyear national strategy to build a cyber resilient Scotland.

David Ferbrache, OBE
Former Chair of the National Cyber Resilience Advisory Board

Measuring impact

The Strategy has four outcomes that contribute to a cyber resilient Scotland. Progress towards these outcomes is measured through a range of national data Indicators, summarised in table 1.

Table 1: Measuring progress of The Framework against national indicators

Strategic Framework Outcomes	Data Indicators	Sources
People recognise the cyber risks and are well prepared to manage them	Percentage of adults taking various security measures online Percentage of adults being confident in pursuing a number of online activities securely	Scottish Household Survey
	Young people's cyber security behaviours and knowledge	Young People in Scotland Survey Young Scot DigiKnow social media campaign
	Older people's cyber security behaviours and knowledge	DigiKen TV adverts Scotpulse surveys
	Number of young people taking part in cyber security learning and skills programmes at schools, colleges and universities	Higher Education Statistics Authority (HESA) SQA statistics
Digital public services are secure and cyber resilient	Public sector bodies incorporating cyber security measures Adoption of ACD measures Participation in Cyber Essentials and Exercise in a Box training Cyber incidents reported under the Notification Policy Use of SG's Cyber Security Procurement Support Tool	Annual Public Sector Cyber Assurance Survey IASME statistics NCSC ACD stats SG CRU stats

Businesses and organisations recognise the cyber risks and are well prepared to manage them	Number of businesses and charities that have suffered a cyber breach Number of organisations accessing Exercise in a Box Growth of cyber security industry Organisations' adoption of Cyber Essentials Mean salary offer and job vacancies for core cyber roles	Cyber Security Breaches Survey 2022 Data from NCSC DSIT Cyber Security Sectoral Analysis SG CRU stats Cyber security skills in the UK labour market
National cyber incident response arrangements are effective	Number of times national plan is tested and exercised	SG CRU annual statistics

The data indicators come from a range of sources including the annual Scottish Public Sector Cyber Survey, the UK Cyber Breaches Survey and the Scottish Household Survey. In most cases we are identifying correlation between the implementation of the Action Plans and positive change in these indicators, but we cannot claim causality. However, in the case of the Scottish Public Sector Cyber Assurance Survey, we are better able to identify a link between national support and impact.

The remainder of this report draws out evidence of progress in five key areas: Scotland's people, public sector, third sector, private sector, and its cyber security industry and skills pipeline.

Section 4: Progress and Priorities going forward

People's cyber resilience

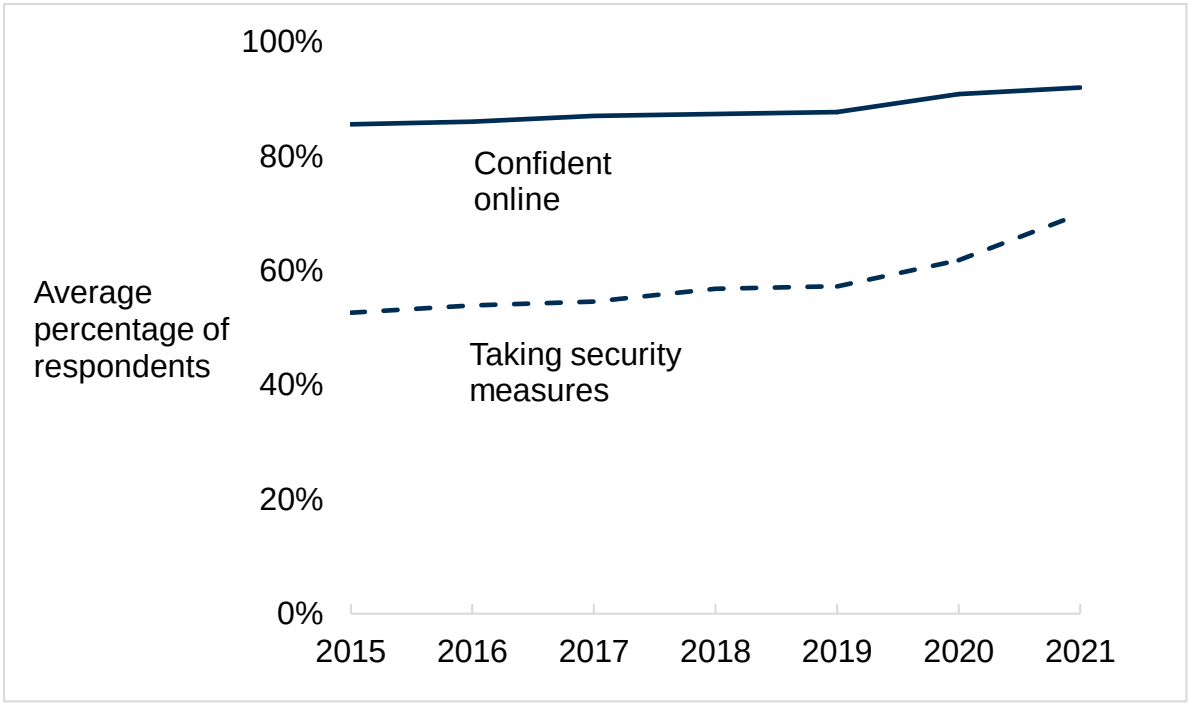
Improved awareness and behaviours

The Scottish Government, working with its partners, oversees a Scotland-wide engagement programme aimed at increasing people's awareness of cyber threats and encouraging better cyber resilient behaviours. This supports our strategic outcome: People recognise the cyber risks and are well prepared to manage them.

Results from the Scottish Household Survey suggest there has been improvement in people's online behaviours. Figure 1 shows that between 2015 and 2019, the average percentage of adults who said they were confident in using the internet increased from 86% to 88%. The average percentage who said they adopt cyber security measures online increased from 53% to 57%.[7]

Data captured from 2020 onwards is not directly comparable with previous years due to the change in survey methods (from face-to-face to telephone based). The 2021 and 2020 data points are therefore separated from the earlier data points in Figure 1. The results from the 2021 telephone survey showed that on average 92% were confident Internet users, and 70% adopted security measures.

Figure 1: Cybersecurity behaviours and confidence among internet users, 2015-2021



Source: Scottish Household Survey

[7] These numbers were calculated by averaging the percentage response across several individual survey questions.

Between 2020 and 2021:

- The percentage of people who said they avoided opening emails or attachments from unknown people increased from 78% to 85%.
- The percentage of people who said they set complex passwords increased from 58% to 66%.
- The percentage of people who said they backed-up important information increased from 58% to 64%.

Reaching diverse groups

The Scottish Government recognises that many people face barriers to communication or require information to be presented in alternative and accessible formats. The Strategic Framework notes that accessibility of cyber advice is vital to ensure that everyone is included, is cyber aware and able to protect themselves online.

The Scottish Government funded the national disabled learners' charity, Lead Scotland, to adapt the NCSC's Cyber Aware guidance into 16 accessible formats, including British Sign Language, Easy Read (for people with learning difficulties) and several community languages. Lead Scotland further disseminated this advice through a series of training sessions for adults. In the feedback, 100% of the participants noted an increase in their confidence levels in improving their own online security.

Cyber resilient behaviour in young people

The 2021 Young People in Scotland Survey included questions about online security. The findings suggest that we continue to face some challenges.

Despite 83% of young people saying they were either 'very' or 'fairly confident' that their online accounts or devices were safe and secure, only 7% stated that they 'never' use the same passwords across different accounts and devices, with 18% stating that they 'always' reuse them. In addition, only 10% stated that they 'always' follow the NCSC's recommendation of using passwords made up of three or more random words. Just one third said they would 'definitely' know where to get help if their online account or device was hacked.

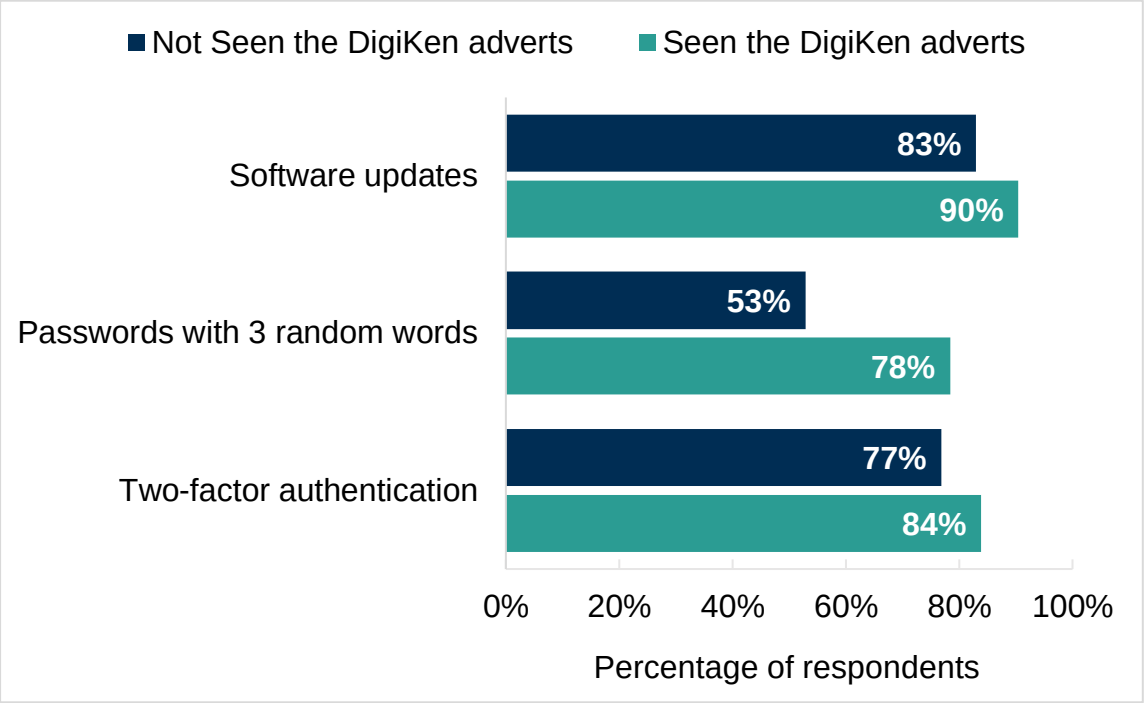
The Scottish Government has funded Young Scot to run an ongoing cyber awareness campaign dedicated to address this gap. Since 2015, this online campaign received 85,462 clicks and 443,113 engagements. In autumn 2022, Young Scot reported that 51% of the young people they surveyed were 'likely' or 'very likely' to secure their accounts by updating their passwords or use a password manager after seeing Young Scot DigiKnow social media adverts.

Cyber resilient behaviour in older people

In 2022 and 2023, the CyberScotland Partnership ran a TV advert campaign for older people, aiming to raise their awareness of basic cyber hygiene. The three DigiKen adverts encouraged people to use passwords with three random words, use two-factor authentication and to update their software and devices regularly.
Credit: Heehaw Ltd

Figure 2 shows that older people who had seen the DigiKen adverts reported higher awareness of the cyber security advice given than those who had not seen the adverts. For example, 78% of people who had seen the DigiKen advert were aware of the advice to use three random words in their passwords, compared with 53% of people who had not seen the advert. This suggests that advertising campaigns can be an effective way of educating the public.

Figure 2: Results from ScotPulse survey on cybersecurity awareness in older people



Source: ScotPulse

However, as with the data regarding young people's behaviour, the ScotPulse survey shows a gap between older people's awareness of the advice and their actual online security habits. For instance, only 26% of those aged seventy and over said they use three random words for passwords.

Looking ahead: priorities for people's cyber resilience

We recognise the wide-ranging impact that digital technologies continue to have on our lives and the importance of a whole of society approach to building cyber resilience. We will be taking further actions in the following areas:

- Increasing the reach and adoption of advice, guidance and support to improve online behaviours of the general public and particularly those who are vulnerable.
- Building the capabilities of the CyberScotland Partnership to ensure wide reach of relevant guidance and support.

The cyber resilience maturity of Scotland's public sector

SG CRU oversees a significant public sector work programme and engages every public sector body in Scotland to support them increase their cyber maturity and resilience. It shares guidance to Scottish public sector bodies for supply chain cyber security (e.g. Cyber Security: guidance for public sector buyers) and to better manage cyber incidents (e.g. Cyber capability toolkit). SG CRU also provides regular, and when required, rapidly arranged engagement through sector-specific networks, workshops and early threat warning notifications. It works with the Digital Office to support local authorities to improve their cyber security. The SC3 fosters collaboration between partners including HEFESTIS (further and higher education), Police Scotland and NHS National Services Scotland (health).

The Scottish Government also coordinates the implementation of the Network and Information Systems Regulations (NIS) to ensure that lessons and good practice from the highly regulated Drinking Water and Health Sectors are shared with the wider public sector.

Assessing the maturity of the Public Sector

The SG CRU conducted a series of surveys of Scottish public sector bodies in 2018, 2019, 2021, and 2023. This report includes evidence from the latest public sector survey and, where relevant, compares it with previous years.

The survey asks public bodies about their cyber security assurance measures in order to gauge their preparedness to manage cyber threats including incident response plans and adoption of Active Cyber Defence (ACD) Measures. ACD refers to the group of cybersecurity services and technologies, introduced by the NCSC, to help organisations deal with the most common but least sophisticated types of cyber threats. The number of organisations that respond varies from one survey to the next and the response rate is never 100%. This creates a limitation in comparing survey results across time, since the results can be affected by which organisations respond to a given survey. However, it does give us a general sense of cyber maturity across the public sector and will help with targeting future interventions and support to specific organisations or subsectors.

The Public Sector Cyber Resilience Framework

The Public Sector Cyber Resilience Framework (PSCRF) provides a consistent structure for Scottish public sector organisations to:

- assess their cyber resilience arrangements
- identify areas of strength and weakness
- gain reasonable confidence that they are adhering to minimum cyber resilience requirements
- make informed decisions on how to achieve higher levels of cyber resilience on a risk-based and proportional basis.

The PSCRF brings together the technical controls from various standards and certifications – including Cyber Essentials, ISO27001, PSN and NIS Cyber Assessment Framework – to form a single framework for the public sector. This allows organisations to compare their cyber maturity with other organisations, regardless of the specific standards an organisation aligns with.

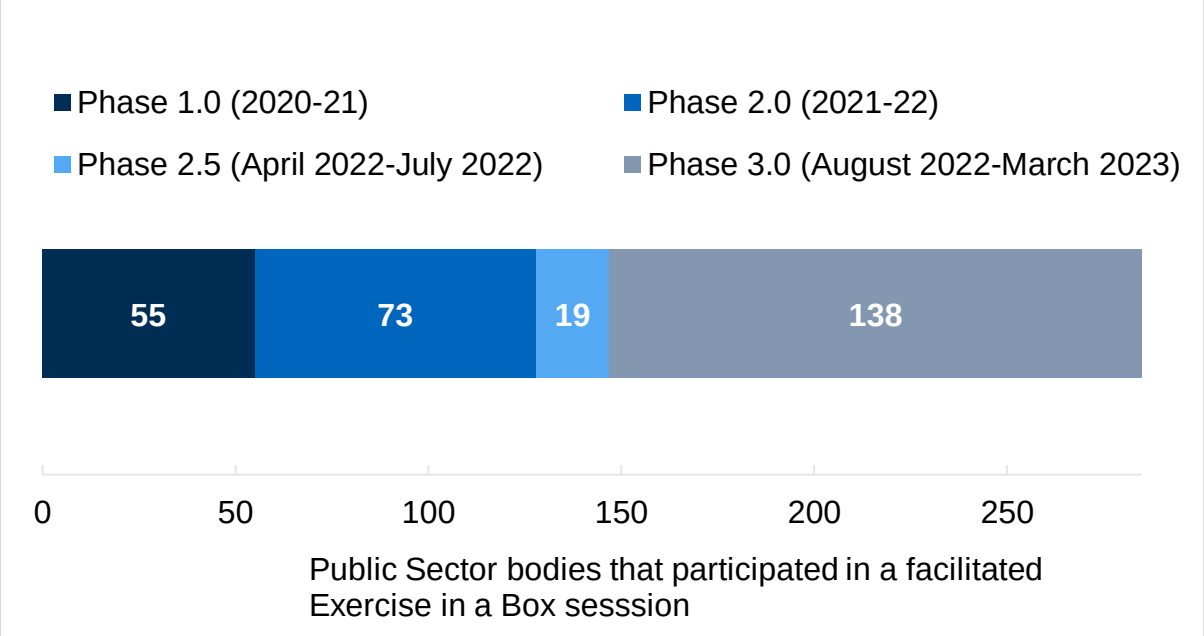
PSCRF adoption is surveyed every year, gauging current levels of capability across a range of areas including cyber assurance, incident response planning and staff training.

Increased incident response planning and exercising

Incident response planning is critical to any organisation's cyber resilience. The SG CRU has provided guidance and training to organisations to develop their incident response arrangements. To embed exercising into organisations' operations SG contracted the Cyber and Fraud Centre Scotland (previously known as the Scottish Business Resilience Centre) to deliver facilitated sessions of Exercise in a Box (EiB) to help public sector bodies practise their response to cyber attack scenarios. Exercise in a Box provides allows organisations to take their first steps into cyber exercising before progressing to more complex and bespoke testing of their plans.

Figure 3 indicates the number of Scottish public sector organisations that participated in EiB sessions over each delivery phase. Fifty-five organisations used EiB during phase 1.0 (2020-21) and 73 used it in phase 2.0 (2021-22). 138 organisations used this tool in phase 3.0 (August 2022-March 2023), suggesting its usage has increased over time.

Figure 3: Number of Scottish Public Sector organisations using Exercise in a Box, 2020-2023

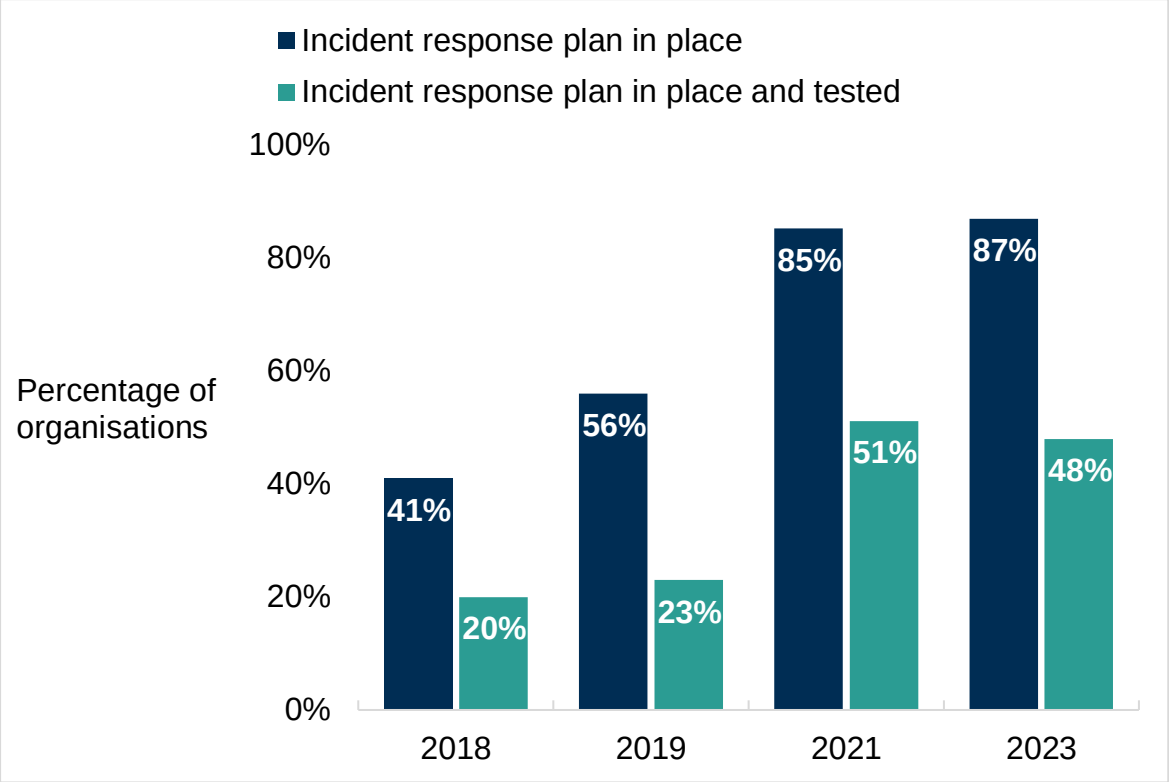


Source: Cyber and Fraud Centre Scotland

There has also been an increase in public sector bodies preparing their incident response plans. Figure 4 shows that the percentage of public sector bodies with an incident response plan in place has more than doubled in 5 years (from 41% in 2018 to 87% in 2023).

However, there is not as much traction with organisations testing their incident response plans and in 2023 only 48% reported that they regularly test their plans.

Figure 4: Percentage of Scottish public sector organisations that have created an incident response plan and have tested their plan



Source: SG CRU

The SG CRU continues to roll out EiB awareness raising sessions and expects a further increase in public sector bodies developing and testing their own incident response plans in the near future.

National exercising underway

As part of the Strategy the Scottish Government is committed to delivering at least one national cyber exercise per year. The national exercise is designed to test inter-agency coordination and linkages with the wider UK cyber incident response arrangements.

Since 2021, the Scottish Government and national stakeholders have exercised various scenarios (including those relating to specific events such as COP26) across various organisational levels (operational to Senior Civil Service and Ministerial levels).

The SG CRU has also supported several local authorities and other public sector bodies with the delivery of bespoke cyber incident exercising.

Public Sector Boards' increased awareness of cyber threat and risk

In 2023, 90% of public sector organisations said they had identified a Board Member or Senior Manager responsible for the organisation's cyber resilience arrangements. This is a slight decrease from the 97% reported in 2018.

To encourage senior executive ownership of cyber resilience, SG has funded the Cyber and Fraud Centre Scotland (previously known as the Scottish Business Resilience Centre) to deliver Executive Cyber Education training to 150 Board Members and Senior Managers. The percentage of bodies with board members responsible for cyber resilience will likely increase further with the roll-out of bespoke Board Cyber Resilience training during 2023/24.

Improved threat intelligence sharing across the public sector

According to the public sector survey, the percentage of organisations using the NCSC's Cybersecurity Information Sharing Partnership (CISP) – a secure online environment for cyber professionals to share and discuss threat intelligence – has increased from 78% in 2018 to 86% in 2021 and then to 89% in 2023. Almost all CyberScotland Partnership's awareness-raising materials and events encourage organisations to join the CISP.

In 2020, the SG CRU created a group within CISP specifically for the Scottish public sector. In 2021, 41% of Scottish public bodies reported they were members of this group. By 2023, membership has increased to 43%. The SC3 will promote the Scottish Public Sector Group on the CISP as a useful conduit for intelligence sharing.

The SG CRU has established a well-respected and widely attended Public Sector Cyber Resilience Network of cyber security professionals from across the Scottish public sector. This forum meets every two months to discuss the latest cyber security developments and shared challenges and it provides a safe space for the sector to share knowledge, lessons and effective practice.

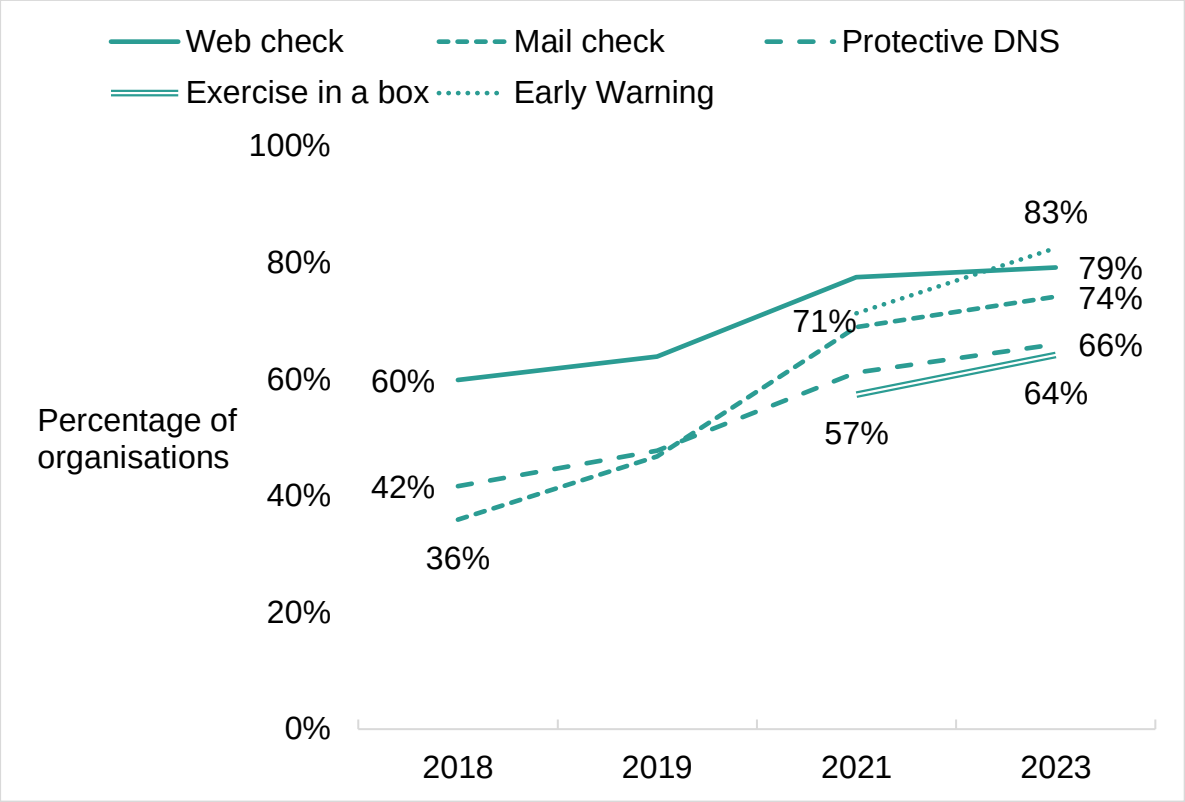
Increased use of Active Cyber Defence Measures (ACD)

The NCSC's Active Cyber Defence (ACD) programme has expanded substantially since its launch in 2017 and provides services to help organisations defend against phishing attacks and to stop public sector systems veering onto malicious servers.

These services include Early Warning, Exercise in a Box, Mail Check, Web Check, Protective Domain Name Service, Suspicious Email Reporting Service and a website Takedown Service. The SG CRU promotes ACD to the public sector and we are now seeing significant increase in the adoption of some of these measures.

For example, the percentage of public sector organisations using Mail Check has sharply increased from 36% to 74% between 2018 and 2023. The trends in ACD use are shown in Figure 5.

Figure 5: Percentage of public sector bodies using Active Cyber Defence Measures, 2018-2023



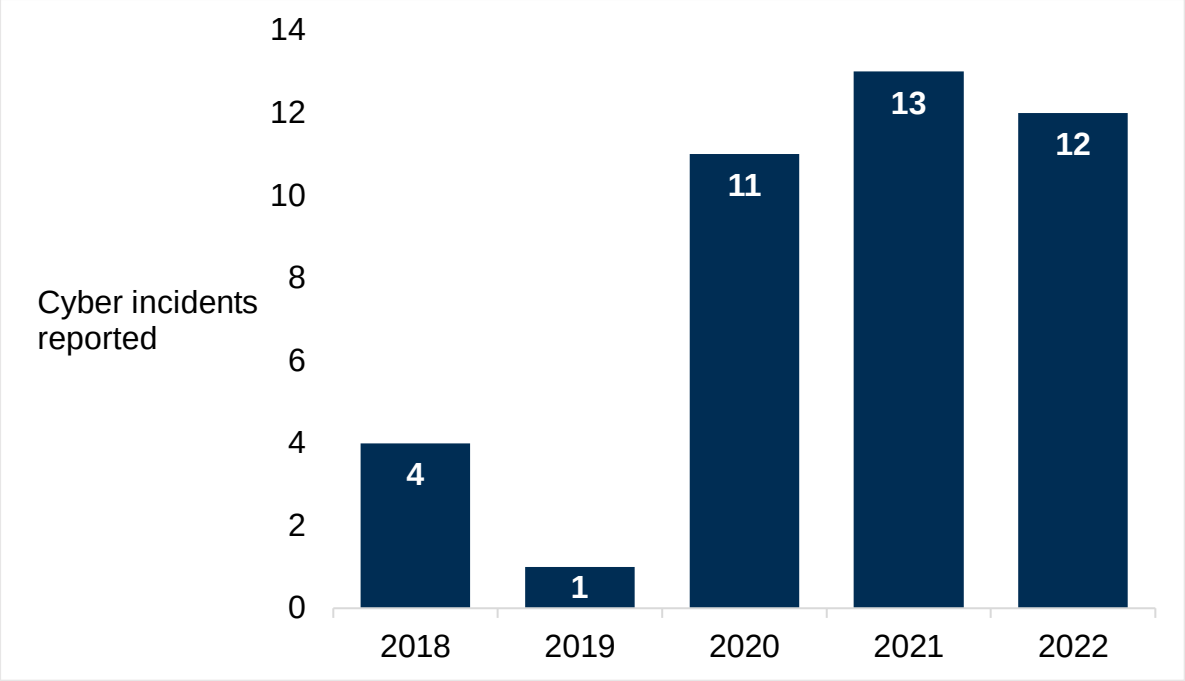
Source: SG CRU and NCSC

Cyber incident notification being used

The Scottish Public Sector Cyber Incident Notification Process encourages the voluntary reporting of cyber incidents to the Scottish Government, Police Scotland and NCSC in a consistent way. This policy helps coordinate a multi-agency response to significant cyber attacks affecting the Scottish public sector and ensures that all necessary resources and expertise can be swiftly deployed to assist organisations during an incident. The SC3 is now taking on the key coordination role for these notifications.

Figure 6 shows an increase in the reporting of incidents through the Notification Policy. Four incidents were reported in 2018 and 12 incidents in 2022. While the Scottish Government is not a reporting agency for cyber incidents, the increased number of notifications may illustrate the strong engagement and trusting relationships between SG CRU and the wider public sector in Scotland.

Figure 6: Number of cyber incidents reported under the Notification Policy, 2018-2022



Source: SG CRU

Independent assurance of critical technical controls

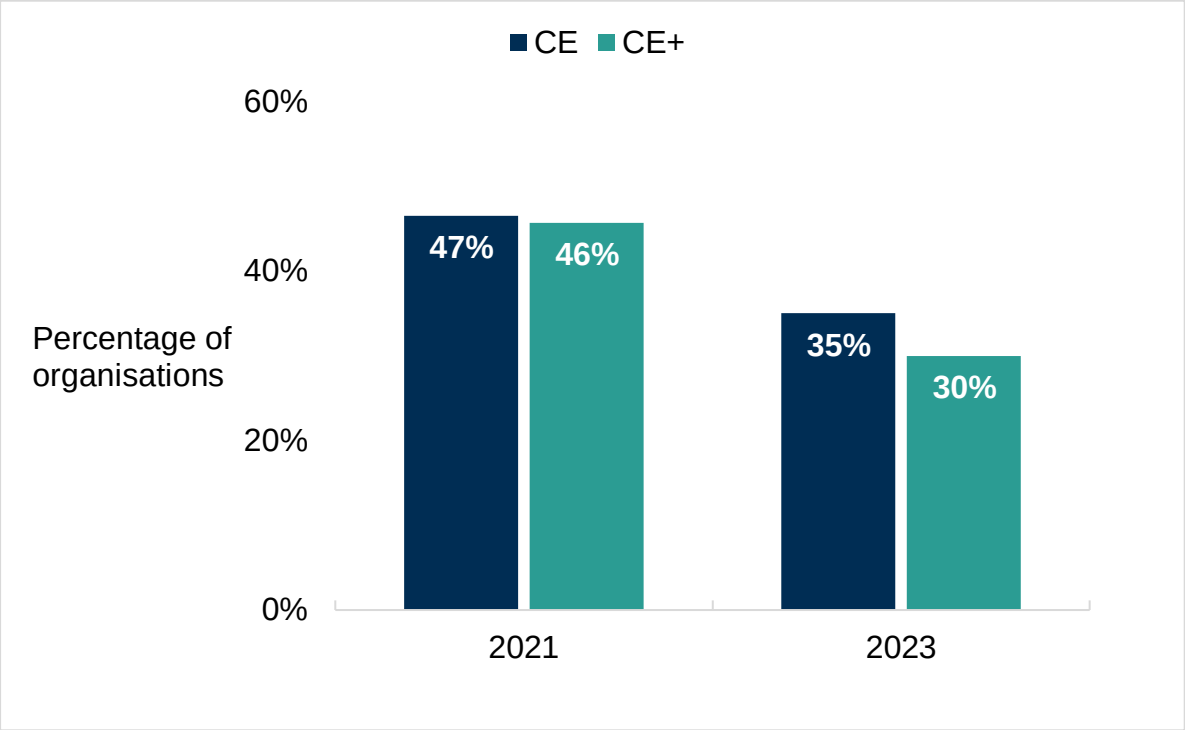
Cyber assurance refers to the systematic evaluation of the security arrangements of an organisation's information systems by measuring how well they conform to a set of established criteria. Scottish Ministers asked all public bodies to put in place arrangements for independent assurance in 2018. They specifically requested that organisations adopt Cyber Essentials (CE) or Cyber Essentials Plus (CE+).

Since then, the number of public sector organisations with CE has decreased slightly over time. In 2021, 47% of organisations had CE and 46% had CE+. In 2023, these percentages had fallen to 35% and 30% respectively as shown in Figure 7.

Possible reasons for the decrease include the significant changes to the Cyber Essentials requirements and assessments which have made the certification more challenging for large, complex organisations to achieve. In addition, some organisations have chosen to pursue other proportionate and risk-based assurance measures more appropriate to their needs, including the PSN Code of Connection.

SC3 has established a workstream to review the cyber assurance landscape across the public sector in Scotland, fully recognising the existing regulatory regimes and essential compliance standards that are already in place, such as the NIS Regulations and the PSN Code of Connection, and the emerging GovAssure process.

Figure 7: Number of Scottish public sector organisations with Cyber Essential certification, 2021-2023



Source: SG CRU

Cyber assurance of the public sector's supply chain

Most organisations rely on suppliers to deliver and provide products, systems, and services. An attack on suppliers can be just as damaging as one that directly targets an organisation. Supply chains can be long and complex, and effectively securing the supply chain can be challenging because vulnerabilities can be inherent, introduced or exploited at any point within the chain.
In 2023, 87% of Scottish public sector bodies reported having cyber assurance in place for their procurement processes. The SG CRU will continue to track progress in this area over time through further surveys and engagement.

Supply chain cyber security and resilience have been central to the Scottish Government's own cyber posture and Scotland's public sector is heavily dependent on the services and products of many SMEs, with more than 19,500 registered with the Supplier Development Programme.

Building on NCSC's supply chain guidance, and to support the Scottish public sector through procurement processes, the SG CRU published supply chain guidance in 2020 and produced a decision-making support tool. The Cyber Security Procurement Support Tool has been providing a consistent approach for the sector to obtain cyber assurance from prospective suppliers as part of the procurement process. Since 2020, the tool has supported 852 organisations (public sector buyers and private/third sector suppliers) with over 1500 registered users. Further work is required to better understand the supply chain eco-system across the public sector.

Developing the cyber security profession in Scotland's public sector

On behalf of the Scottish and UK governments, ScotlandIS delivered funding of £145,000 to upskill 85 cyber security professionals from 30 public sector organisations during autumn 2022. These organisations included 17 local authorities, 12 health boards and one other organisation delivering essential services.

Aligned with the UK Government, the Digital, Data and Technology (DDaT) Profession was introduced within the Scottish Government to attract and retain the talent required. In Scotland, the DDaT Profession includes an additional family of jobs with common definitions for Cyber Security and Information assurance roles and this lays the foundation for standardisation of roles and clearer career paths across the wider public sector.

Since autumn 2021, the Empowering Women to Lead Cyber Security in Scotland programme (run by Empowering You) has been supporting the professional development of women in cyber-related roles across the public, private and third sectors with creative, highly experiential workshops, individual coaching and a group-led challenge presentation. To September 2023, 107 women have graduated . Further cohorts will graduate in 2024.

Credit: Empowering Women to Lead Cyber Security: Empowering You

Building cyber resilience awareness of the general workforce

Since 2017, with funding from the Scottish Government, Scottish Union Learning has worked with 24 unions and 132 organisations across both the public and private sectors to deliver cyber security and resilience training for employees engaging within 3,793 employees. In addition, Scottish Union Learning has trained 259 union learning representatives.

A toolkit for workers developed as part of the programme has been used over 2,500 times and the four video 'lessons' have been used 500 times. Workers do not have to be members of a union to participate in training.

Looking ahead: priorities for the public sector

For the foreseeable future, supporting the growth of the public sector's cyber resilience maturity will remain a priority for the SG CRU team, with a particular focus on:

- Setting agreed targets for specific areas of the public sector and collaborating with our partners to deliver activity that will improve the rate of exercising, adoption of Active Cyber Defence measures, log retention policies and supply chain management.
- Developing and implementing a cyber assurance regime for the public sector to highlight gaps and make improvements in their cyber resilience. It will be necessary to better understand the supplier chain eco-system across the public sector and better identify cyber security gaps and needs.
- Supporting public sector bodies to identify the most appropriate standards with which to align and the cyber assurance mechanisms that verify them.
- Developing cyber security professional skills within the public sector, including supporting the work of the UK Cyber Security Council to raise professional standards.
- Strengthening the role of the Scottish Cyber Coordination Centre (SC3) to support the public sector with early warning, intelligence sharing, exercising and incident response coordination.

The cyber resilience of Scotland's third sector

The Department for Science, Innovation and Technology's (DSIT) Cyber Security Breaches Survey (2023) suggests that despite being more aware of the NCSC's guidance than businesses, third sector organisations are less cyber resilient than businesses across the UK.

Almost a quarter of UK charities have identified a cyber breach in the past year. 31% of charities have board members or trustees with responsibility for cyber security, an increase from 26% recorded in the 2022 survey. However, there has been a decline in the percentage of charities that consider cyber security as a priority at a senior level. This has decreased from 72% to 62% over the previous year. This is a particular concern for low-income charities (under £100,000 in annual income) because they experienced an even bigger decrease from 67% to 53%.

Differing cyber resilience maturity across the third sector

With the relatively low cyber resilience maturity level in many parts of the third sector, the SG CRU commissioned an academic research project to look at the opportunities and challenges. It has provided recommendations which, together with the findings of a series of engagement sessions with the sector, will help inform the direction of future work.

Building cyber resilience within the Social Care sector

The Scottish Council for Voluntary Organisations (SCVO) has led the way in the third sector to raise awareness of the cyber risk, helping organisations understand their cyber maturity level, their risk levels and the steps they can take to manage these risks.

Two priorities were identified within the SG CRU's third sector work programme (2021-23):

- Social care – due to the potentially severe impact of a cyber incident which could put lives at risk, and the sensitive nature of the data held.
- Housing – due to the housing sector's overlap with the social care services and its notable funding responsibility.

Social care is delivered by organisations from all sectors and professional development for carers is provided not only by employers but also by the Scottish Social Services Council (SSSC). The SSSC is in its third year of engagement activity dedicated to growing the capacity of care providers, including in the third sector, to help their staff to be cyber resilient, and to improve the cyber resilience of service users, many of whom rely on digital technologies for accessing public services, but also for everyday activities like shopping and communication.

The SSSC has included cyber resilience as part of its online learning offer, which is freely available on their staying secure online webpage.

From August 2022 to July 2023, 78 third sector organisations took part in the facilitated Exercise in a Box sessions. The priority social care and housing organisations are included in future targets for the delivery of the Exercise in a Box.

Looking ahead: priorities for the third sector

The complex composition of the third sector in Scotland is posing a significant challenge in terms of understanding its cyber resilience capabilities and posture. The extensive range of sizes, sub-sectors, delivery mechanisms and causes they work towards also creates challenges in effectively using the right approach.

A 2023 research report Cyber resilience and the third sector – risks, challenges and opportunity: research report commissioned by the Scottish Government provided an analysis of the sector, its needs and attitudes towards cyber resilience. It also identified the following challenges:

- Lack of consistent advice, guidance and regulations in key areas of cyber resilience and security
- Low level of experience and knowledge of cyber security and resilience amongst Board members
- Unsuitable UK cyber certification requirements for some areas of the third sector
- Cyber security and resilience complex language and terminology
- Insufficient funding for cyber resilience development generally.

The Scottish Government and the CyberScotland Partnership will address these challenges and work closely with third sector national representative bodies, including SCVO as the lead organisation to establish the best support model to improve cyber resilience across this sector.

The cyber resilience of Scotland's private sector

DSIT's Cyber Security Breaches Survey 2023 shows that:

- 32% of businesses reported a cyber incident, which was slightly fewer than in the previous two years.
- Around one third of the businesses surveyed had board members accountable for cyber security as part of their role.
- The finance and insurance, health and social care, and the information and communications sectors generally have better cyber security and resilience postures than other sectors.

Risk awareness

Scotland is a nation of small and medium-sized enterprises (SMEs), with SME's employees accounting for 44 per cent of total Scottish employment and 38 per cent of turnover, according to the Small Business Survey Scotland (2021). The survey also found that smaller businesses invest less in cyber security and resilience measures.

As part of the Private Sector Action Plan, a range of events and training have been offered to the private sector in Scotland. These have included Exercise in a Box training to 276 businesses (between April 2021 and June 2022), Executive Cyber Education to senior leaders (2021-22) and ongoing support to companies through the Internet of Things (IoT) Secure Services initiative encouraging a secure by design approach to the development of IoT (in 2022-23). The Scottish Government also funded the Cyber and Fraud Centre Scotland to operate a free helpline for the SME community and the third sector to help victims of cyber crime understand what support is immediately available to them and assist them with recovery. Since April 2021, it has supported 134 organisations (including 97 private sector businesses) in Scotland.

Cyber Essentials

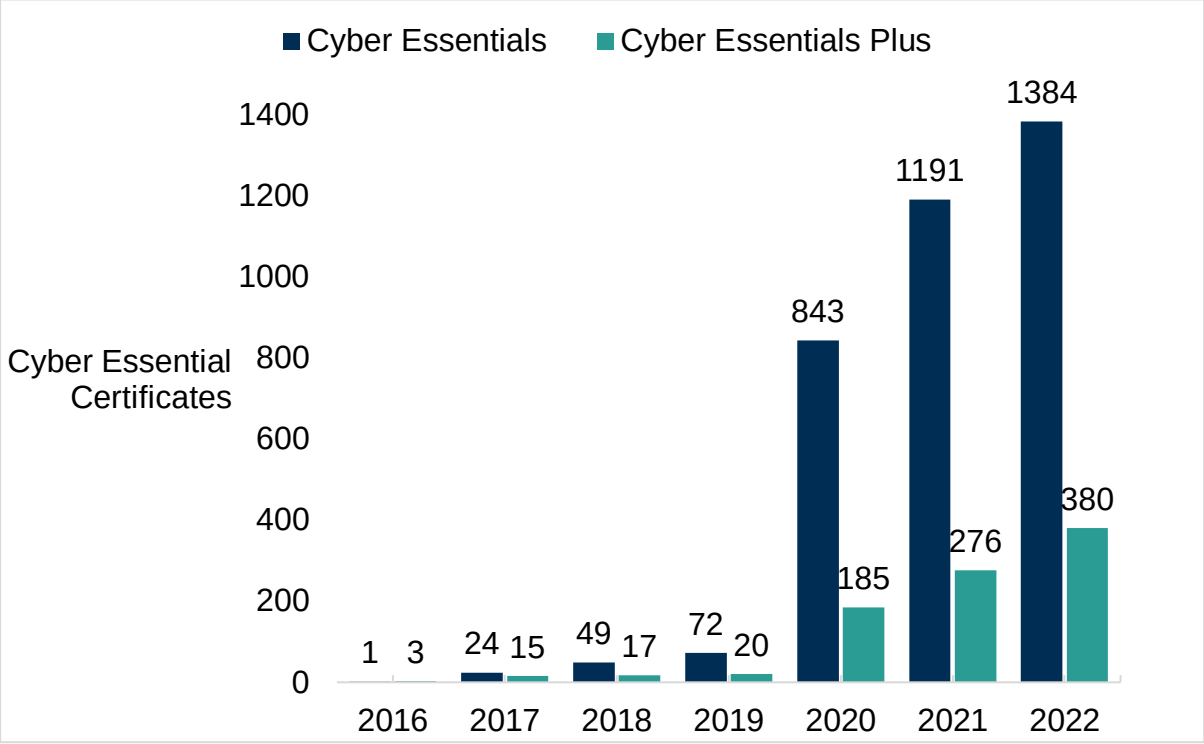
In 2015, the Cyber Resilience Strategy for Scotland positioned the Cyber Essentials scheme as an important baseline standard of security, protecting organisations against the most common, non-targeted cyber attacks.

IASME is the NCSC-nominated authority for managing the Cyber Essentials scheme. Both IASME and the NCSC are key stakeholders in the Cyber Scotland Partnership supporting the collaborative approach to securing a cyber resilient Scotland.

The rapid adoption of Cyber Essentials (CE) and Cyber Essentials Plus (CE+) among all Scottish organisations is demonstrated in Figure 8. The number of CE certifications increased from 1 in 2016 to 1,384 in 2022. The number of CE+ certifications increased from 3 to 380 over the same period.[8]

[8] An organisation which certifies to CE+ receives both a CE and a CE+ certificate. A breakdown between public and private sector bodies is not available, but the majority of these organisations are private sector.

Figure 8: Cyber Essentials certificates issued to Scottish organisations in each year, 2016-2022



Source: IASME

Key Influencers / IT Managed Service Providers (ITMS)

In 2021, 40% of businesses in the UK used an IT Managed Service Provider (ITMS), and in the Cyber Breaches Survey it was found that the cyber security aspect was not an important consideration to businesses when selecting a Managed Service Provider (MSP).[9] Many businesses assumed that the ITMS also looked after the cyber security for their company, which in the case of some suppliers was a misconception.

Since then, the SG CRU has worked with ScotlandIS to map out both the Cyber Security and IT Managed Service Providers in Scotland. Two searchable directories are now available online of Scottish cyber security companies and IT Managed Services.

This work identified that many of the ITMS providers were themselves small businesses, looking after the interests of predominantly other small businesses. Half of them appeared to lack any cyber security certification. ScotlandIS engaged with the ITMS and 47 organisations have gained Cyber Essentials or Cyber Essentials Plus certification so far, thus improving understanding of risk and client expectations around incident response.

[9] Department for Digital, Culture, Media & Sport, Cyber Security Breaches Survey 2022 (2022)

Recognising ITMS' role as a critical touchpoint for cyber security to small and micro businesses, ScotlandIS further engaged with the ITMS to bring them together as a network of organisations to facilitate knowledge and share expertise, with the aim of improving the cyber security of their clients.

DigitalBoost Development Grant

The Business Gateway DigitalBoost Grant distributed Scottish Government funding to businesses and organisations to help them use digital technologies and enhance workforce skills.

With the SG CRU's efforts, a condition of the grant allowed the successful applicant to undergo a cyber health check in the form of a Cyber Essentials Pre-Assessment. Since 2021, at least 3,320 businesses have undergone the Cyber Health Check placing them in a better position to understand the cyber threat and risk to their business and pointing them to mitigations available to reduce this risk.

Looking ahead: priorities for supporting the cyber maturity growth of the private sector

Scotland's business landscape consists of almost 360,000 small and medium enterprises, and they account for over 99% of all private sector businesses[10]. Engaging with them all effectively remains a challenge and it will be necessary to target those business areas most at risk of a cyber attack, or most vulnerable if subject to an attack. Utilising business representative bodies/touchpoint will also be useful routes to businesses.

Whilst policy interventions proved effective at some key points for pockets of the private sector, they have not been yet performed at a scale that could significantly improve the businesses' understanding of risk, their organisational security or preparedness at the national level.

More collaboration between the public and private sectors is required. Areas of focus will include:

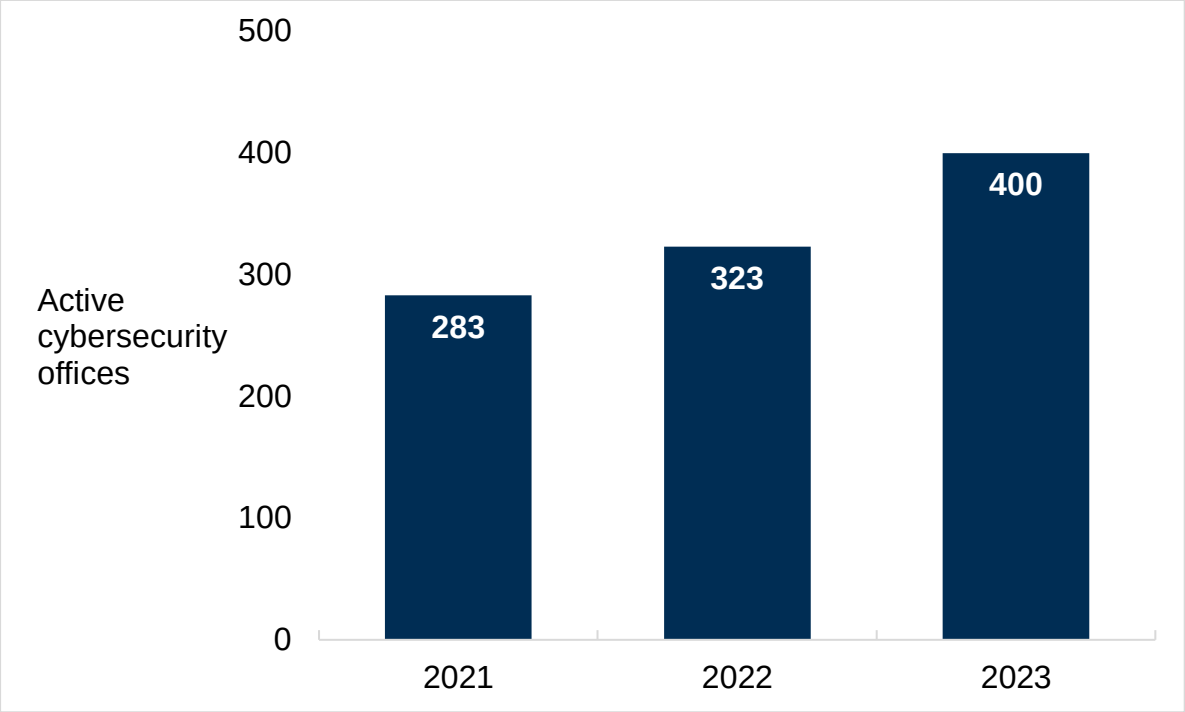
- Through SC3, building collaboration and sharing threat intelligence and solutions through private and public partnership
- Promoting the secure by design approach to our industries, and in business use of technology
- Closing the skills gap and engendering a cyber resilient culture across Scottish businesses.
- Working with business representative bodies to extend reach to businesses.

[10] Scottish Government, Businesses in Scotland: 2022 (2022)

Building the cyber security industry in Scotland, and growing the skills and the talent pipeline

The Scottish cyber security products and services industry is growing steadily, and the number of active cyber security offices reached 400 in 2023, as shown in Figure 9.

Figure 9: Number of active cyber security offices in Scotland, 2021-2023



Source: Cyber Security Sectoral Analysis 2023

Scotland maintains its position within the growth of the wider UK cyber security sector:

- In 2022, Scotland was home to 8% of the active UK cyber security offices and hosted approximately 7% of all the UK-based cyber security employment – the same as in 2021[11].
- Scotland had 2,338 core cyber security job vacancies in 2022
- Scotland had the third highest percentage (13%) of all UK core cyber security job vacancies in 2022[12] out of twelve UK regions. In 2021 this figure was 5.3%[13].
- The mean salary offer for these vacancies has dropped from £56,800 in 2021 to £54,500 in 2022, which may be accounted for by the economic climate.

[11] UK Government, Cyber security sectoral analysis 2023 (2023)
[12] UK Government, Cyber security skills in the UK labour market 2023 (2023)
[13] UK Government, Cyber security skills in the UK labour market 2022 (2022)

The maturity of Scotland's cyber security education ecosystem

In 2022, the NCSC assessed the maturity of the cyber security education ecosystems of a number of areas in the UK, including Scotland. Scotland was classified as "dynamic" in twelve areas including:

- our key educational establishments
- our certified degrees
- our cyber security cluster
- our careers network
- our numbers of Higher and Advanced Higher Computer Science pupils and the growth in the number of female students for these awards (though it is acknowledged that numbers are still low).

  NCSC's report identified areas for continued improvement, including in relation to the numbers of students studying for Higher National Certificates and Diplomas in colleges, and the numbers of female students at all levels.

Skills shortage

As with most countries, the cyber security industry in Scotland and the rest of the UK faces skills shortages to meet the increasing demand. According to the 2023 Cyber Security Skills in the UK Labour Market survey[14], 44% of employers in the cyber sector said that the job applicants they have seen lacked technical cyber security skills.

The 2023 survey (which refers to the labour market in 2022) found that:

- An average of 5,921 core cyber roles were advertised each month in the UK. 7% of these were located in Scotland[15], which is an increase from 5.3% in 2021.
- There were an estimated 7,000 new entrants into the UK cyber security workforce, with 4,700 estimated to have left the sector.
- There was an estimated shortfall in personnel in the cyber security sector of around 11,200 people in 2022. This is a decrease from 2021 where the shortfall was an estimated 14,100.
- There is still a low number of the workforce coming from diverse backgrounds.

In response to the continuing skills shortage, the Scottish Government has set out key actions relating to skills development in its Learning and Skills Action Plan and works with Skills Development Scotland, Education Scotland, the NCSC, Scotland's colleges and universities, the Abertay cyberQuarter and other partners to strengthen the skills pipeline and meet demand.

[14] UK Government, Cyber security skills in the UK labour market 2023 (2023)
[15] UK Government, Cyber security skills in the UK labour market 2022 (2022)

Development of cyber security professionals

The cyber security profession is relatively young and with the increasing demand for cyber security professionals, many people occupying cyber security roles lack qualifications or professional certification, having developed their knowledge and skills while in the role and over a number of years on the job.

DSIT's Cyber Security Skills in the UK Labour Market 2022 report shows that 39% of employers specified in their vacancy adverts that they expected candidates to hold a Certified Information Systems Security Professional (CISSP) certification. This request was an increase from 36% in the previous year, and the demand for other certifications is also increasingly common.

The UK Cyber Security Council is the self-regulatory body for the UK's cyber security profession. It is responsible for agreeing and putting in place nationally recognised standards for cyber security. The Scottish Government hosted a roundtable for the Council's leaders to meet Scottish stakeholders in October 2022, following which the Council was invited to become the seventeenth partner in the CyberScotland Partnership, where it will be well placed to work with partners to embed standards in Scotland.

To formalise the skills of professionals working in the sector, ScotlandIS have managed upskilling funding on behalf of the Scottish Government. Since 2021, it has provided 335 cyber security staff across 103 Scottish organisations in all sectors with financial support to enable them to undertake a variety of certifications, and we note there is a clear appetite for further similar opportunities.

Talent attraction - careers awareness, creating opportunity and promoting diversity. Awareness of cyber security careers – especially of the plethora of rewarding roles available and how to get into a role – remains low. Gender balance is still an issue with women accounting for 23% of the workforce in digital technology roles.[16]

Greater diversity in the workforce means that problem solving can be richer and more creative and it is a practical step towards filling the skills gap. We are not attracting enough people from diverse backgrounds into the cyber security profession, and we are not seeing career progression with these groups. Boards and senior management in particular tend to lack diverse background representation. The Scottish Government has taken steps to address this by funding activity that promotes cyber careers to people living in disadvantaged communities, supporting neurodivergent people through training, and offering mentoring to women to become confident leaders, and they see this a priority going forward.

The CyberScotland Partnership has been working hard to inspire young people and career changers, and to promote pathways into careers. It will continue to focus on reaching people who face barriers, not only to feel confident to begin training in cyber security and to enter the profession, but to progress once they are in work.

[16] ScotlandIS website, Diversity and Inclusion

Skills Development Scotland has led cyber careers awareness through their Digital World website[17], where it hosts information about roles in the profession and provides information about where to find courses and undertake qualifications. Since 2017 it has delivered 33 online "Live Lessons" on several topics relating to cyber security, aimed at 12- to 14-year-olds, and has reached nearly 20,000 pupils. And their online independent lessons have been accessed 372,361 times since 2017. SDS is also coordinating industry engagement in education through its Tech Education in the Classroom programme, which brings together employers and equips them to support young people's skill development and aspiration. This programme seeks to link and maximise the impact of existing programmes, including STEM Ambassadors and ScotlandIS's Critical Friends programme.

YouthLink Scotland, the national youth work agency, has been working to embed cyber resilience and awareness of cyber security careers into youth work programmes, and Young Scot has showcased careers in the cyber industry to young people directly through its DigiKnow? information campaign and on social media.

A creative and innovative programme by Civic Digits CIC theatre company has included interactive performances of The Big Data Show that has, to date, reached more than 3,000 students from P7 to S3. 830 students have received an award in "An Introduction to Basic Cyber Resilience and Digital Citizenship" at SCQF level 3. Civic Digits are now working with the cyberQuarter and industry partners to deliver immersive one day experiences at the cyberQuarter for P7 children from Dundee.

Big Data Show, CyberScotland Week 2022. Credit: Aly Wright

CyberFirst in Scotland

In March 2023, Education Scotland signed a Memorandum of Understanding with the NCSC to be the CyberFirst partner for Scotland, with the aim of growing the programme in Scotland and improving schools' and colleges' capacity to deliver high quality cyber security learning and teaching. A pilot saw seven schools recognised as CyberFirst schools. The CyberFirst Girls Competition, which seeks to inspire girls

[17] Digital World website, Become a Digital Human

to consider training and careers in cyber security, has grown in popularity in Scotland, with 65 schools taking part in 2023 (up from 29 in 2022).

Stirling High School, CyberFirst Girls Competition (Scotland) winners (2023). Credit: NCSC

Qualifications and vocational training

Scotland has developed a comprehensive and coherent framework of cyber security qualifications from school-age to PhD, and numbers of learners have been increasing..

Cyber resilience and security qualifications available in Scotland (May 2023)			
SCQF Level 12	PhDs		
Level 11	Masters Degrees	Graduate Apprenticeship in Cyber Security (Masters)	
Level 10	Honours Degrees	Graduate Apprenticeship in Cyber Security (Honours)	PDA in Cyber Resilience
Level 9			PDA in Cyber Resilience

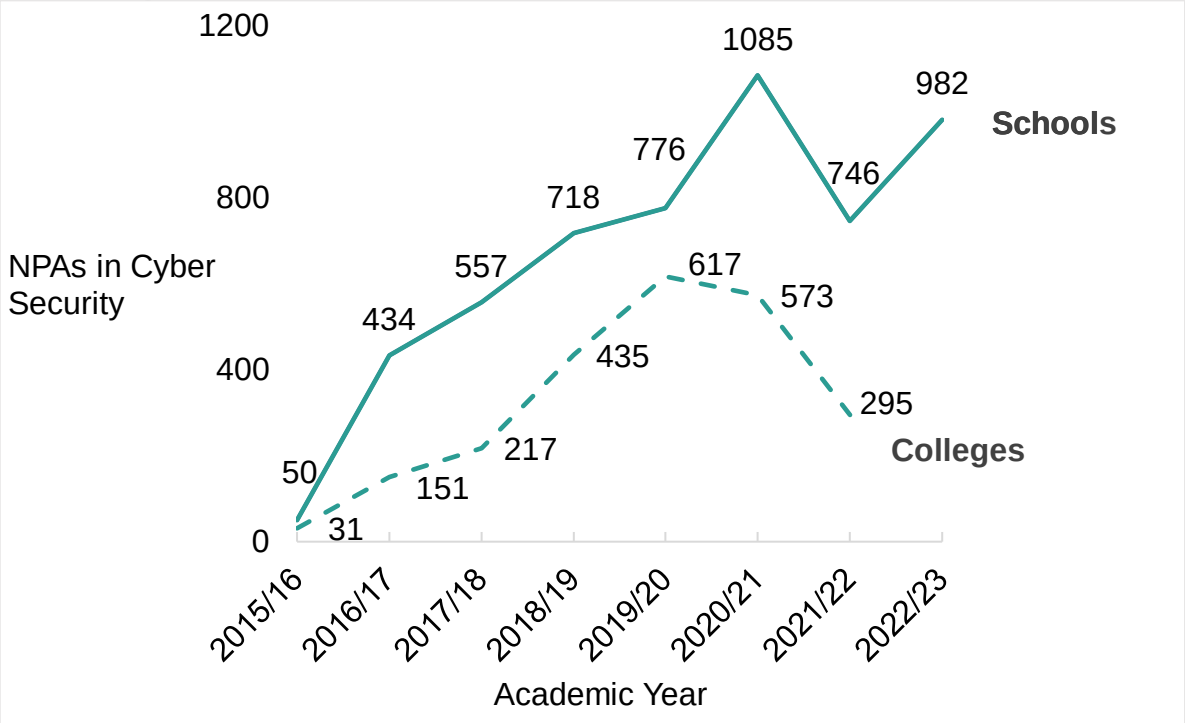
Level 8	SQA Higher National Diploma (HND)	Modern Apprenticeship in Information Security	
Level 7	SQA Higher National Certificate (HNC)		PDA in Cyber Resilience
Level 6	SQA National Progression Award in Cyber Security	Modern Apprenticeship in Information Security	
Level 5	SQA National Progression Award in Cyber Security		
Level 4	SQA National Progression Award in Cyber Security	SQA Cyber Security Fundamentals Unit	SQA Internet Safety Unit

National Progression Awards in Cyber Security

The SQA's National Progression Awards (NPA) in Cyber Security were launched in 2015. They are available at Scottish Credit and Qualifications Framework (SCQF) levels 4, 5 and 6 and are delivered in schools and colleges. More than 100 of Scotland's secondary schools deliver the NPAs, of which the most popular is the level 5 qualification.

By the academic year 2022/23, 5,348 pupils had taken an NPA in cyber security, with numbers of entries increasing year on year, with a lull caused by the pandemic. Numbers of female students remain low, but they are increasing year on year. 19 colleges deliver the NPAs, with the level 5 again being the most popular. By the academic year 2021-22, 3,018 students had taken an NPA in college. These trends are highlighted in figure 10.

Figure 10: National Progression Awards (NPA) in Cyber Security in schools and colleges, 2015/16 to 2022/23

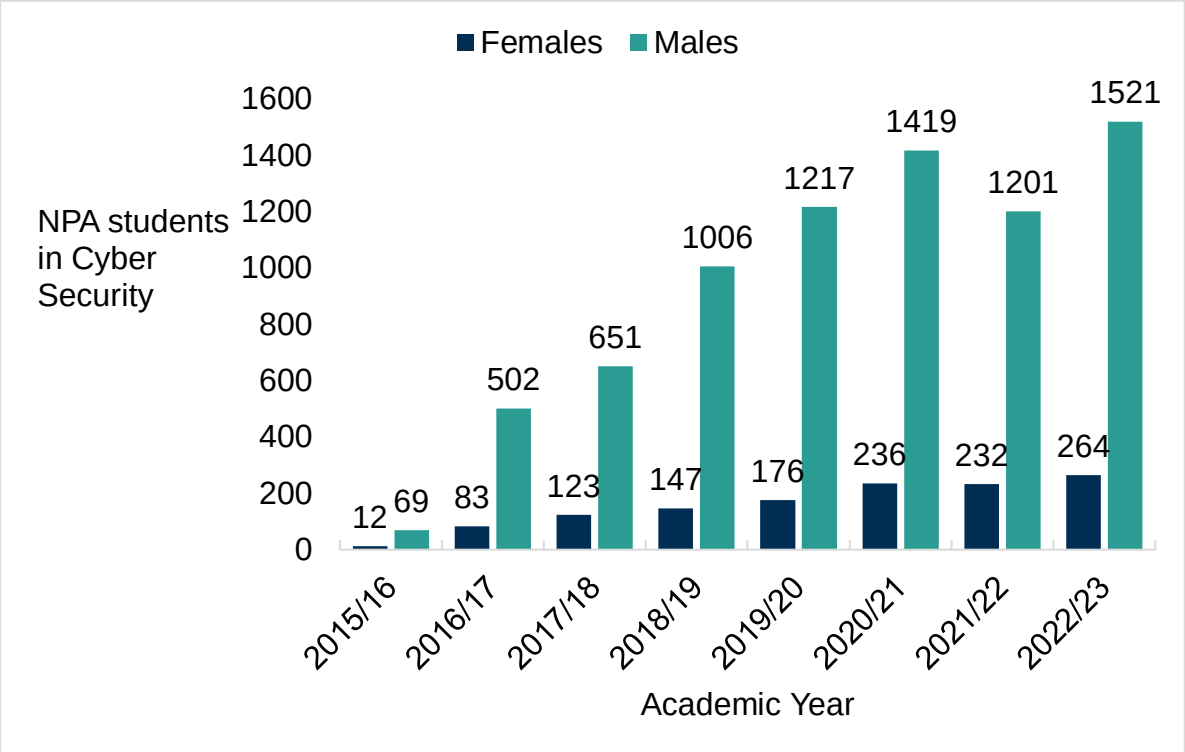


Source: Scottish Qualification Authority

Gender disparities

Figure 11 shows the numbers of students taking an NPA in cyber security at SQA levels 4, 5 and 6, from the 2015/16 academic year to the 2022/23 academic year. Numbers have increased year on year, except in 2021/2022 when the COVID-19 pandemic caused some students to defer their studies. There is a large gap between female and male students. In 2022/23 there were 1,521 male students and 264 female students in these courses.

Figure 11: National Progression Awards (NPA) in Cyber Security, males and females, 2015/16 to 2022/23



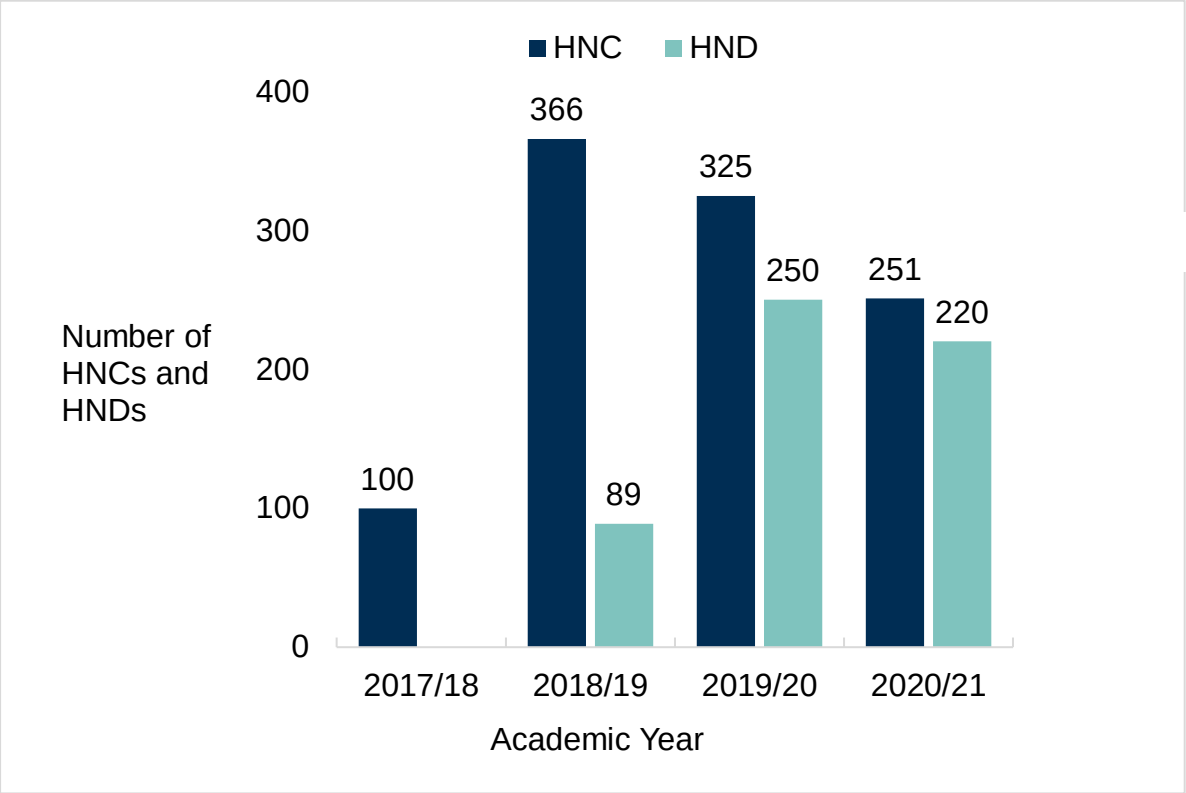
Source: Scottish Qualification Authority

The proportion of female students has remained low over time, and in total only 14.4% (1,273) of all those achieving the award (8,859) over time were female.

Higher National qualifications

Eleven colleges deliver Higher National (HN) qualifications in cyber security. These are available at Certificate (SCQF level 7) and Diploma (SCQF level 8). Some colleges have “articulation” agreements in place with universities, whereby students can use their HNC or D to move directly into the second or third year of a degree programme. Since its launch in 2018, 1,317 students have studied for the HN Certificate. Since its launch in 2019, 738 students have studied for the HN Diploma. These trends are highlighted in figure 12.

Figure 12: Higher National Qualifications and Diplomas in Cyber Security, 2017/18 to 2020/21



Source: Scottish Qualification Authority

Degrees

Thirteen universities offer degrees in cyber security, or degrees in computing that include modules on cyber security. The number of undergraduates increased from 5,265 in 2019/20 to 5,745 in 2020/21. The number of postgraduates increased from 1,500 in 2019/20 to 2,050 in 2020/21.

Graduate Apprenticeships

Honours-level Graduate Apprenticeships are offered by three universities, with Masters-level offered by a further three. Between its launch in 2017 and the 2021/22 academic year, 195 students had enrolled in an honours-level apprenticeship. Between its launch in 2018 and the 2021/22 academic year, 177 students had enrolled in a Masters course.

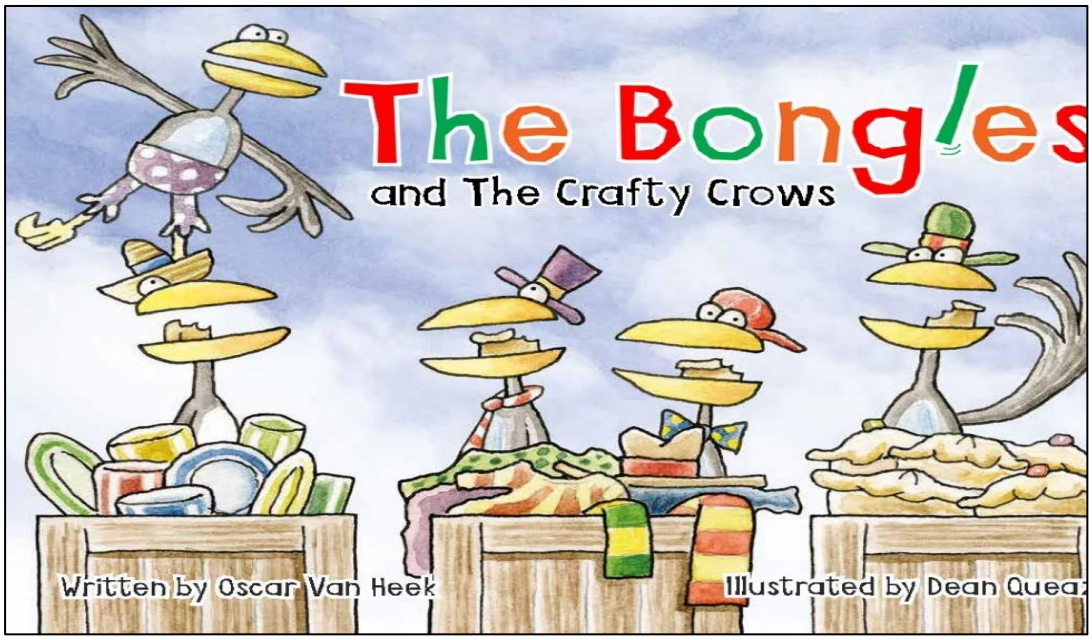
Places are heavily skewed towards male students, with the percentage of male students consistently over 80% each year to date.

Looking ahead: priorities for the cyber security sector and for skills

- The Scottish Government will continue to work with partners to boost upskilling activity, to enable cyber security professionals, especially in the public sector, to gain new skills and certification.

- The Scottish Government and its partners will work together to increase our efforts to promote diversity, working with multiple partners to deliver the inaugural cyber-related diversity summit in autumn 2023. This will be followed by an action plan focused on empowering people who face barriers to entry or progression in cyber careers.
- The CyberScotland Partnership will continue to encourage the cyber industry to support cyber security learning in schools, colleges and universities.
- The Scottish Government and its academic and education partners will encourage continued growth of cyber security courses in further and higher education as well as embedding cyber security and resilience within other academic disciplines.

We want to equip teachers and parents of the youngest children with high quality resources to ensure children learn the fundamentals of cyber security. The Scottish Government and Education Scotland are launching *The Bongles and the Crafty Crows*, a storybook for first-year primary school children, which focuses on learning outcomes relating to security, passwords and passcodes. It will be distributed to all 54,500 Primary 1 children in November 2023, in time for Scottish Book Week and will have associated learning and teaching materials available for teachers. NCSC have endorsed the book.



Source: The Bongles and the Crafty Crows

Next steps

The Scottish Government and its partners will continue to work together to realise Ministers' vision of Scotland thriving as a digitally secure and resilient nation. Refreshed action plans will be published in the Autumn of 2023 to build on progress made so far and to continue our work towards a safe, secure and resilient future for Scotland.

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: 978-1-83521-481-7 (web only)

Published by The Scottish Government, October 2023

Produced for The Scottish Government by APS Group Scotland, 21 Tennant Street, Edinburgh EH6 5NA
PPDAS1371554 (10/23)

w w w . g o v . s c o t