POLICY AND STRATEGY

Cyber action plan for Wales

How we will help people, businesses and public services reduce the risks of cyber-attacks and build a thriving cyber economy.

First published: 3 May 2023

Last updated: 3 May 2023

Contents

Ministerial foreword

Introduction

Priority area 1: Grow our cyber ecosystem

Priority area 2: Build a pipeline of cyber talent

Priority area 3: Strengthen our cyber resilience

Priority area 4: Protect our public services

Ministerial foreword

The challenges of the past few years have shown us the importance of digital in our lives. Digital tools and technologies are now often central to the way we learn, work, access public services and do business. Our reliance on digital, however, has also led to a stark increase in the risk of cyber-attacks which are becoming ever more common and sophisticated. We are in an age where this threat mutates so quickly, we need to work on the basis that cyber-attacks will happen. Our businesses, organisations and public services must take steps not only to reduce the risks but to prepare for, deal with and have plans in place recover as quickly as possible from any incident.

While the cyber resilience and security of people, businesses and public services must be at the core of our participation in a modern digital world, cyber also offers great economic opportunities for Wales.

Our Programme for Government is clear, we want to build a stronger, greener, economy based on the principles of fair work, sustainability and the industries and services of the future. Cyber is both an enabler and a risk in supporting us to achieve this.

Wales is leading some of the most interesting and innovative work on cyber. We have one of the biggest cyber ecosystems in the UK and we are already home to global players in the cyber industry. Our universities have created centres of excellence and are producing world-class research and talented graduates with specialist skills the sector demands.

We have a great story to tell and this Cyber Action Plan starts to tell it. Wales has already made significant investments in cyber and this plan sets out a consistent and coherent strategic direction for the future. It sets out our intent to maximise the benefits of our investments through collaboration, strengthening partnerships and building on our previous work. We are doing a lot in Wales and we should celebrate the real progress we have already made. This plan is about consolidating our gains and it is clear to see how we will advance as government and as an ecosystem.

The Cyber Action Plan is driven by our values as a nation; a place of fairness; social justice and providing opportunities for all to participate in what accelerating technological change brings to the future of work and society.

Being a small, connected country with close relationships makes us agile and by strengthening and advancing our competitive advantage we can reap economic opportunities. Through delivering this plan, with an emphasis on partnerships and shared goals and ambition, we will capitalise on our existing strengths and activity and ultimately make Wales more prosperous and resilient for now and future generations.

Vaughan Gething MS
Minister for Economy

Introduction

In an age where we are more digitally connected than ever, online services and digital technologies touch almost every aspect of our society. For most people they are essential to day-to day life, they support the growth of our economy and enable the running of essential infrastructure.

The **Digital Strategy for Wales** sets a vision of improving the lives of everyone through collaboration, innovation and better public services. Effective cyber defence and resilience, a strong cyber business sector and people, businesses and public servants who are cyber aware are crucial to achieving this.

For the purposes of this plan, “cyber” has multiple meanings. It means that everyone feels confident to be as safe as possible online. It means our businesses are as productive, efficient and resilient as possible and our public services are effective and trusted by the people who use them. It also means enabling the longer-term transformation of the Welsh economy through nurturing the industries of the future and a skilled digital workforce to support it.

The increased use of digital services poses opportunities, challenges and threats. The global risk of cyber-attacks is rising alongside the exponential pace of technological advancement, and Wales is not immune. This is evident from high profile cyber-attacks over the last few years such as the attack on the SolarWinds IT management platform – which resulted in a major and complex, global cyber incident – and the ransomware attack which took offline multiple NHS health systems, including the NHS 111 service.

The risk of cyber-attacks brings the possibility of disruption to individuals, organisations and businesses. While no system can be made totally secure from the continually mutating threat of a cyber-attack, we can take steps to reduce the risk and be prepared to deal with and recover from any incident. For organisations and businesses, it is far more than an IT issue. It is vital leaders understand, and have planned for, the significant potential impact of a cyber-attack.

Understanding and harnessing the power of cyber is critical not only to our ability to be as resilient as we can be but to also achieve the ambitions of the Digital Strategy for Wales. A thriving Welsh cyber sector which attracts global investment will support a prosperous economy. This is underpinned by access to the right cyber skills and knowledge for organisations, industries and businesses through attracting and developing those skills in Wales.

This Cyber Action Plan complements a number of other relevant strategies such as the UK Government **National Cyber Strategy** 2022 and its **Government Cyber Security Strategy** 2022 to 2030. We continue to play a role in the collective effort to support the delivery of these strategies through membership of groups which oversee their implementation. While distinct and different, we must also think about where this plan crosses over into the wider context of how we keep people safe online and we will continue to seek a partnership approach with the UK Government on these matters.

We also work closely with the National Cyber Security Centre (NCSC) and our counterparts across the UK and the National Cyber Advisory Board (NCAB) and will continue to do so to achieve our vision and to make sure Wales' voice is heard.

Future generations

This Cyber Action Plan will contribute to our progress towards the national well-being goals and Well-being of Future Generations (Wales) Act.

Embracing digital and cyber innovation will lead to greater economic opportunities and a more prosperous society. Building on the strong partnerships referred to in this plan will develop new innovations, new jobs and new skills where they are needed.

Growing digital and cyber skills, across all age groups, will help us as a nation take advantage of technological change for work and society. It will lay the foundations for everyone to participate to build a more equal Wales.

Ultimately, when people, businesses and public services understand both the risks and opportunities associated with cyber and digital services, we will build a stronger and more resilient Wales for the future.

We will promote and protect the Welsh language as part of the delivery of this plan, including working with the UK Government to ensure it takes account of our needs in the delivery of its policies and services.

Our vision

Our vision for cyber in Wales is:

> “ Wales prospers through cyber resilience, talent, and innovation. ”

In practice this means that people, businesses and public services are as secure and prepared against cyber-attacks as they can be, that we have the right skills and workforce to support the ambition in this plan and we have in place a thriving cyber economy supported by world class research. These are not mutually exclusive and need to work together to deliver our vision.

How we will achieve our vision

This action plan sets out how we will achieve our vision for cyber in Wales. We will focus on four priority areas to help us do this. These are:

- Priority Area 1: Grow our cyber ecosystem
- Priority Area 2: Build a pipeline of cyber talent
- Priority Area 3: Strengthen our cyber resilience
- Priority Area 4: Protect our public services

The four priority areas are interlinked and interdependent. For example, partnerships between industry and academia can help with understanding of the impacts of cyber-attacks on businesses and public services. In turn, that fosters the creation of new cyber companies in Wales to provide solutions which support the growth of our economy. Such innovation also makes Wales an attractive place for businesses to invest and locate their businesses and to feel secure in doing so.

To do all of this we need the right skills, not only by developing home grown talent but having unique opportunities in Wales to make it a place where cyber professionals want to stay. Innovation, a strong cyber sector and a skilled cyber workforce ultimately makes Wales a more secure and resilient nation.

These parts form a Wales 'cyber ecosystem'. This plan and vision are cross-cutting and bound together by building a culture of cyber awareness.

Who is the Cyber Action Plan for?

This Cyber Action Plan is primarily for organisations and industry. It is also designed to encourage collaboration between industry, academia, government, wider public services, Arm's length bodies and law enforcement.

Ownership, accountability, and review

While we, the Welsh Government, have a clear leadership role, alongside UK Government, in the delivery of this action plan, we cannot achieve this alone. It requires a whole of society approach and the collective efforts of public services, industry, academia, law enforcement and government at a local, national and UK level including Arm's length and sponsored bodies.

As a devolved government we can consider the public policy levers available to us, however, the success of this plan depends on more than those levers in isolation. To deliver this action plan we must embrace partnership working, collaboration and coordination across sectors; breaking down existing silos to reach our ambitions.

As the Welsh Government we will review and monitor this action plan and publish updates on progress. We will also work with partners to establish ways of measuring this plan.

Priority area 1: Grow our cyber ecosystem

Use cyber as an engine for economic growth by harnessing our strong partnerships and reputation for innovation

The Digital Strategy for Wales sets out our aim to drive economic prosperity and resilience by embracing and exploiting digital innovation.

Our investments and partnerships across academia and industry to date have helped to build Wales' reputation as a place where the cyber sector can innovate and thrive. It is underpinned by a vibrant Small and Medium Enterprise (SME) community and cyber clusters of excellence, with clear links between large multinationals, academia, SMEs and Government. The ecosystem we have in Wales helps draw on our home-grown talent, bringing fresh ideas and new ways of thinking into the market and supports SMEs to flourish.

What we are already doing

Our **International Strategy** identifies cyber security as one of three distinct and growing sectors in which Wales has expertise, experience and ambition and we are already home to many of the global players in the cyber industry. We are using the competitive advantage of our already thriving cyber security sector to attract new inward and foreign direct investment into Wales. We are prioritising relationships with international networks which will enable us to share our cyber experiences and learn from others, participate in collaborative cyber projects and enable cyber businesses in Wales to grow their exports as well as create opportunities for companies to invest in Wales.

We have already directly awarded investment of £3 million in the **Cyber**

Innovation Hub. This is alongside £3 million from Cardiff Capital Region and a further £3million from Hub partners. The Hub, led by Cardiff University, brings together industry, government, defence and academic partners to grow the Welsh cyber security sector. It is creating a coordinated approach to skills, innovation and new enterprise. It will train more than 1,500 individuals with cyber security skills, create more than 25 high growth companies, and attract more than £20 million in private equity investment by 2030. It will help attract and anchor the best cyber security talent so that we create high quality jobs in Wales and in the industries of the future. The Hub will deliver bespoke training to provide industry and public services with the skills they need.

We have developed a partnership with Airbus Defence and Space (based in Newport) and Cardiff University (on behalf of universities in Wales) through the Endeavr programme. The programme invites application from SME's and academia in Wales to support projects that address technology challenge areas within Airbus Defence and Space thus increasing capabilities within Wales and embedding these technologies within the Airbus supply chain.

One of the projects developed by Endeavr has led to the Airbus Centre of Excellence in Human Centric Cyber Security which is creating a human-centric analysis with technical expertise.

As part of the Tech Valleys Programme for Government commitment, we have committed over £12 million to support the National Digital Exploitation Centre (NDEC) until 2025 in collaboration with Thales UK and the University of South Wales. The NDEC is a Cyber Security Centre of Excellence, leading the development of digital trust and security in operational technology environments. It also provides research and development, education and outreach and SME support.

Alongside this, the Welsh Government has committed £3.5m for the delivery of ResilientWorks via a partnership between Thales, industry and academia in collaboration with Cardiff University and EyzOn Energy. ResilientWorks is an innovative, collaborative environment providing open access testbeds for developing technologies for electric vehicles and connected autonomous vehicles (CAVs) and the associated charging/energy infrastructure.

The NDEC and ResilientWorks sit alongside each other, forming the Thales Ebbw Vale Technology Campus. The Campus is also the global Cyber Operations Technology Centre for Thales.

What we will do next

Together, we will:

- maximise our investments and partnerships with industry and academia to grow our cyber ecosystem, build cyber skills and bring benefits to Welsh public services
- develop Wales’ reputation as a safe and secure place to do business and raise our profile internationally as a place where cyber security companies can innovate, grow and thrive.

Priority area 2: Build a pipeline of cyber talent

Attract, develop and retain the cyber skills we need by cultivating cyber talent from school age through to the workforce

To grow our cyber ecosystem and to support the safety of people, businesses and public services, we need the right skills in Wales. The Digital Strategy for Wales articulates our aim to create a workforce that has the digital skills, capability and confidence to excel in the workplace and in everyday life and is supported and trained to deliver confidently in a digital environment.

While cyber security companies need skilled professionals, all organisations which use digital services need to consider cyber and have access to the right skills and leaders at all levels need to be cyber aware. To attract, develop and retain those skills, a clear understanding of the requirements of the cyber profession is needed.

Whilst formal and school age education is important, life experience and wider, transferable skills can bring many benefits to a career in cyber. Maximising the opportunities to re-train and cross-skill individuals can help to address the skills needs of sectors in the shorter term, while exploring the end-to-end cyber education journey will help us build the longer-term pipeline of talent.

While we can foster and develop skills at any age, the need to attract and retain those skills in Wales is equally as important.

We all have a responsibility to ensure that our talent pipeline is strengthened by supporting a more diverse and inclusive cyber ecosystem. This plan will help to tackle barriers to accessing cyber or wider STEM opportunities and support under-represented groups.

What we are already doing

Building the pipeline of cyber talent and entrepreneurial spirit starts with our education system. Engaging and motivating children from a young age to develop their interest in Science, Technology, Engineering and Maths (STEM) subjects can set foundations to grow that interest into a career.

Wales already has a strong track record and reputation for cyber skills.

Our **Curriculum for Wales** gives digital competence the same emphasis as numeracy and literacy. It also helps learners understand how technologies and systems work alongside the broad legal, social and ethical consequences of using technologies and systems. Digital competence is a mandatory cross curricular skill within the Curriculum for Wales. All schools and settings must develop a curriculum which enables learners to develop digital competence and capability. Learners are expected to develop and apply these essential skills across all areas of the curriculum.

We provide resources to support our learners to develop basic cyber skills through our national digital learning platform**,** Hwb, and engaging schools with wider UK programmes such as CyberFirst and Cyber Explorers. The CyberFirst Schools programme enhances cyber security IT skills and we have worked with the Tech Valleys funded NDEC education outreach programme, the University of South Wales and the NCSC to implement a pilot project for schools in Wales. The pilot project was initially rolled out in the Tech Valleys region and is now being expanded pan Wales in conjunction with Technocamps and hubs at the University of South Wales, Bangor University, Swansea University and NDEC.

Initiatives like Cyber College Cymru are helping to prepare students for a career in cyber with industry specific training from experts in the field. This is in addition to numerous existing cyber security apprenticeship courses, offering a hands-on approach to careers in cyber.

Many Welsh universities offer undergraduate and postgraduate taught programmes in cyber security. Cardiff University is recognised as an Academic Centre of Excellence in research and education in cyber security. The Welsh Government works closely with the NCSC to enhance higher education links with key employers which, combined with world-class research and development opportunities, makes Wales an attractive place for students to study and follow a pathway into a career in cyber.

Our employability programmes, including ReAct+, Jobs Growth Wales+ and Community Employability Programmes can be used to support cyber skills courses for people of all ages. Personal Learning Accounts (PLA) also offer courses and qualifications to help employed people upskill and reskill in priority sectors, including cyber, to strengthen their position in the labour market and improve career and earnings prospects. Our Flexible Skills Programme (FSP) provides a joint investment with business to incentivise employers to increase investment in the skills development of the workforce.

As well as enabling the growth of our cyber ecosystem, our investments in the Cyber Innovation Hub and NDEC are further supporting the skills agenda in Wales. The Cyber Innovation Hub offers a unique and coordinated approach to skills, innovation, and new enterprise creation while the education and outreach activity carried out by the NDEC enhances local skills and knowledge.

Primary and secondary schools are already doing more to make learners aware of careers options and create real-world learning experiences. Businesses must be willing to help keep abreast of their own changing needs and work in collaboration to provide learners with opportunities to learn about the skills valued in the workplace.

The percentage of women within the cyber profession needs to increase and Wales already sets strong example with one of the most active 'Women in Cyber clusters' in the UK and Europe. Our Equality in STEM Board, chaired by the Minister for Social Justice, provides strategic direction to improve equality in STEM-related study and careers in Wales. We have provided almost £1.5 million in grant funding to support the delivery of STEM initiatives with a strong focus on encouraging girls to consider careers in STEM. This includes funding for Technocamps, which deliver computer coding workshops to pupils and teachers in every secondary school in Wales. We also actively participate in the NCSC's annual CyberFirst Girls Competition which is designed to inspire interest in technology careers and increase uptake of Computing GCSE subjects by female students.

What we will do next

We will bring together industry, academia and public services to leverage the collective opportunities afforded by the activity happening across Wales.

Together, we will:

- explore ways to maximise existing activity in the development of an end-to-end cyber education journey that aligns with modern cyber career frameworks
- participate in the development of professional cyber career frameworks and take into account best practice for public services
- maximise our partnerships and retraining programmes, such as our Jobs Growth Wales+, ReAct+, Personal Learning Accounts and Flexible Skills Programmes, to address the need for cyber skills in the short and longer term for the sectors that need them and support people of all ages into a career in cyber
- use our existing programmes and work with industry partners and schools to improve the diversity of the cyber workforce in Wales, building on the success of interventions such as the Women in Cyber Wales cluster and Cyber First Girls initiative.

Priority area 3: Strengthen our cyber resilience

Keep our people, businesses and whole nation resilient against cyber threats

Being cyber resilient means that people, organisations and businesses can prepare for, detect, respond to and recover from cyber-attacks. It is fundamental to achieving our vision, to our economic goals and to our national security.

The more resilient our businesses are to cyber threats, the more resilient the supply chain is for all. It means Wales' businesses can thrive, taking full advantage of the benefits of digital with confidence and in turn it supports the growth of our cyber eco system.

For people, reducing cyber risks means supporting them to be safe and legal online, with confidence at all ages. Around 7% of adults in Wales still lack the digital skills needed to make full and confident use of online services, with digitally excluded people being some of the heaviest users of health and social care services. See: **Digital inclusion in Wales**. We must ensure that everyone has the knowledge and understanding of good cyber security practices to protect themselves from risks and enable them to fully engage with the benefits offered by the internet.

For businesses, it means understanding and being prepared for cyber threats in order to be as productive and efficient as possible. Different sectors need to understand how cyber affects their distinct circumstances and to foster a culture of awareness and preparedness. Access to the right cyber support and accreditation is crucial to developing more secure Welsh businesses. It will be important to place a particular emphasis on sectors of strategic importance to Wales, such as manufacturing, which employs circa 150,000 people and contributes around 16% of our national output.

The industries that run our key services, such as telecommunications (both mobile phone and fixed broadband), energy, water and transport industries have a central role to play in cyber resilience and the protection of essential infrastructure. Interruption to this infrastructure could cause serious disruption, endanger people's lives and potentially damage the economy.

As services like transport evolve to rely more and more on interconnected digital systems, they also face an alarming increase in cyber-attacks. Those systems must be protected against the deliberate or accidental compromise of confidentiality, integrity or availability, that might put them, and the services they enable, at risk.

What we are already doing

Crimes occurring when people use online services (often called cyber-crime) can cause significant harm to individuals and businesses. This is why we work with Welsh Police Forces, Regional Organised Crime Units (ROCUs) and UK partners on the prevention of cyber-crime. Fostering these relationships has enabled inward and outward loans with key partner agencies, ensuring Welsh Government is at the forefront of cyber resilience and providing leadership in threat intelligence collection and dissemination. This will allow for dynamic expertise on cyber incident management, particularly on ransomware threats - a significant threat faced by UK organisations.

We work closely with the NCSC and the Wales Cyber Resilience Centre (WCRC) to provide the latest advice on cyber security to businesses through our Business Wales digital channels and advisory services. We are also working with targeted sectors, such as the legal and social care sectors with the aim of maximising the reach of those efforts and provide a sense of how different sectors can optimise cyber resilience. From our key strategic partnership with industry bodies, a number of Welsh law firms have committed to secure the NCSC’s Cyber Essentials+.

In partnership with the Regional Cyber Crime Unit (RCCU), Tarian, there is focus on further improving the cyber resilience of essential infrastructure in Wales. This is a targeted effort to provide these sites with NCSC recognised certifications and accreditations, both for the sites themselves and individual staff. Transport is an important part of our essential infrastructure and we are working with key partners such as Transport for Wales to ensure that Wales' transport network is resilient; from our public transport networks to ports, maritime and aviation.

We are working to reduce digital inequalities and supporting people to become digitally confident. Our **Digital Communities Wales**: digital confidence, health and well-being (DCW) programme works with organisations best placed to reach those facing digital inequalities and provides training and support to front line staff and volunteers on being safe and legal online. DCW works closely with key organisations including the University of South Wales, the National Cyber Security Academy, police forces and their cyber-crime teams and community safety officers to ensure training and support is consistent for everyone.

We provide guidance and resources for schools and parents to equip children and young people with excellent knowledge, skills and strategies to keep safe and secure online through **Hwb**. We are working with a range of partner organisations to enhance digital resilience provision, policy and practice as part of the Wales-wide **Digital Resilience in Education Action Plan**. Some children and young people have been trained to become “Digital Heroes” and are confident in using digital while staying safe online.

We also support ROCUs in their wider work, for example with their 'Prevent' work aimed at steering young people away from cybercrime by channelling their cyber skills into positive activities.

We will continue to work with the NCSC to promote their “Cyber Aware” campaign to help provide people with information on how to stay secure online.

What we will do next

Cyber resilience sits at the foundation of this plan and is everyone’s responsibility. We will use our strong partnerships to build a culture of cyber awareness and preparedness for individuals, organisations and our nation as a whole.

Together, we will:

- influence and actively promote the latest cyber advice from the National Cyber Security Centre and other partners such as the Wales Cyber Resilience Centre, including working with NCSC to ensure bilingual advice is available.
- maximise our partnerships and existing mechanisms to help everyone stay as safe as possible online, especially those people most disadvantaged.
- support organisations across sectors in Wales to strengthen their cyber resilience through training and partnership working
- ensure Wales' voice is heard in matters of national security and that we are prepared to protect our nation against cyber threats

Priority area 4: Protect our public services

Our public services and third sector are as safe, secure and resilient as they can be, with an embedded culture of cyber awareness

The Digital Strategy for Wales commits to transforming digital public services so that they are modern, efficient and designed around user needs. Cyber security and service resilience should be a key consideration when services are designed and delivered.

Keeping our public services as secure as they can be is about more than just provision of online services. It also includes the operational technology (OT) that keeps those services running, for example providing access to buildings, managing fire alarms and operating lifts. Increasingly, public organisations are using Internet of Things (IoT) technology and Artificial Intelligence (AI) in public service delivery and will need to become familiar with the cyber security implications that come with it.

To deliver safe, secure and trusted digital public services we must grow and encourage a culture where cyber is everyone's business, from leadership to front line. The impact of a cyber-attack on public services cannot be underestimated, it can shut down the core day-to-day activity of an organisation and severely disrupt the ability to deliver essential services. It is a real threat as illustrated by the zero-day ransomware attack on **Copeland Borough Council**. The attack, which shut down much of the council's digital systems, took over a year to recover from with costs in the millions of pounds as a result.

Leaders must be prepared with plans to help detect attacks, recover from them and minimise their impact. IT and cyber professionals need the skills and everyone in an organisation must be aware of and actively working in ways to reduce cyber risks. It is therefore imperative that public services continue to invest in cyber security, technology and take steps to reduce the risks and to prepare for, deal with and recover from any incident.

Taking a consistent approach to cyber will help strengthen our resilience. Through collaborating with others, as One Welsh Public Service, we can work with common purpose and principles to protect our public services and improve the quality, effectiveness and sustainability of those services for the people of Wales.

Organisations, regardless of their sector, need to be aware of and manage cyber security risks and protect against cyber-attacks. They also need to be able to detect cyber security events and minimise the impact of any cyber security incidents. When incidents do occur, they need to be resilient and recover quickly. They need to embed disaster recovery planning in business continuity management activities and learn from those incidents.

While public services face certain challenges when it comes to cyber, we are working collaboratively to learn lessons and build consistency, and across sectors with academia and industry to address these challenges in new and innovative ways.

Public services can use their influence, investments and public policy levers to help strengthen the resilience of our businesses for example, by setting out the minimum standards they expect in procurement of services or as a condition of funding.

Specific sectors, such as health, energy, transport, digital infrastructure, and water are subject to the **Network and Information Systems** (NIS) Regulations. These UK wide regulations aim to raise the level of cyber security and resilience of key systems and came into force in 2018. In Wales, Welsh Ministers are the **Competent Authority** on implementation of the regulations for health whilst regulation of our water industry is delegated to the Drinking Water Inspectorate.

The UK Government intends to update the NIS regulations to boost security standards and increase reporting of serious cyber incidents to reduce risk of attacks causing disruption. They can also be updated in the future to cover new organisations or sectors if they become vital for essential services. The implications of any future changes to the regulations for Wales will need consideration.

What we are already doing

We are creating CymruSOC', a Cyber Security Operations Centre (SOC) for the Welsh public sector, firstly encompassing Local Authorities and Fire & Rescue Services. It will bring these services, together with Government, the NCSC, and a specialist Managed Service Provider (MSP), to collectively detect and respond to threats and engage in shared incident handling.

CymruSOC is a first of its kind solution to cyber resilience taking a 'Defend as One' approach which will build a joined-up public sector stance. It will link to other Welsh SOCs - with strong working relationships pursued with those of the Shared Resource Service (SRS), the Senedd, and Digital Health and Care Wales (DHCW). It has support from NCSC as part of their 'Securing

Government' work assisting Government entities across the UK.

Continuing in this shared vision of defending together, industry experts are supporting us in the delivery of a Fusion Cell, and the Welsh Warning, Advice and Reporting Point (WARP). Both groups are designed to reinforce local authority resilience and draw upon input and guidance from the NCSC. The Fusion Cell enhances the response to minor incidents while the WARP allows for information sharing on threats, incidents and solutions.

There is now an All-Wales Cyber Technical Advisory Cell (CTAC) which can be stood up in anticipation of, or in response to, a particular cyber threat. It comprises of expert volunteers from such sectors as police and health as well as industry, that can provide critical advice to Strategic Coordinating Groups (SCGs) on responding to incidents and reduce harm. Alongside this we are refining Incident Management (IM) playbooks for use by the public sector to identify gaps and issues in response capability

We are continuously exploring how to support the cyber resilience of Welsh organisations, offering a range of targeted Local Authority funding to enhance their resilience level. This includes providing additional funding to ensure they have Security Information and Event Management (SIEM) solutions in place.

To further build consistency across public services, we are working with Local Authorities to pilot the implementation of the NCSC's Cyber Assessment Framework (CAF). Designed to help organisations achieve and demonstrate appropriate cyber resilience levels, this framework is in use within organisations critical to essential infrastructure and is being piloted across UK Local Authorities.

The CAF Enabling Programme aims to equip leaders, audit/risk professionals and IT professionals with the knowledge and understanding to fully utilise the CAF for their organisation's benefit. In addition, the programme will look to establish a network for professionals involved in the CAF to share good practice and to work collaboratively to improve cyber resilience.

At an awareness level, training on cyber security is carried out across public service organisations in Wales to support their knowledge and ability to recognise and respond effectively to potential cyber risks. We also facilitate delivery of industry specific training for the Welsh public sector, with bespoke cyber security training for elected councillors, cyber resilience seminars and training videos for social care, and data breach workshops and guidance for Local Authorities.

The Centre for Digital Public Services (CDPS) will also be highlighting the importance of cyber security and resilience as part of its digital leadership offering.

Training alone is only one intervention to support organisations with their cyber resilience which is why we also facilitate activity such as the NCSC's 'Exercise in a Box', Not2Phish and specific targeted exercising.

We have mandated standards for Welsh Government Sponsored Bodies and encouraged adoption by other Arm's-Length Bodies in Wales to provide assurance that the services that they deliver are secured to reduce risk and to enable them as organisations to recover from incidents.

To support the implementation of the NIS Regulations we have funded and established a Cyber Resilience Unit (CRU) for the NHS in Wales which undertakes operational responsibilities to assess against the requirements of the NIS Regulations. We have published **statutory guidance** on how healthcare providers in Wales should implement the NIS regulations. This was supported by a baselining exercise for health in Wales to identify key findings and remediations in four areas; managing cyber risk, protecting against cyber-attacks, detecting cyber security events and minimising the impact of cyber security incidents.

What we will do next

The success of this Cyber Action Plan relies on collaboration and a strong, joined-up, cyber-aware public service is ultimately a safer one. We have already made significant investments in cyber which is growing our ecosystem in Wales. Our next step is to harness the benefits of this for public services so that we can build skills and act as a test bed to drive forward solutions.

Together, we will:

- define and help embed consistent standards to deliver safe and secure digital public services
- support public services to strengthen their cyber resilience and preparedness, underpinned by collaborative working and information sharing supported by the design and delivery of a Cymru SOC.
- provide the leadership needed to encourage and foster a culture of cyber awareness across public services from the top down
- leverage the benefits of our investments in cyber innovation to support public services with the challenges they face when it comes to cyber
- support public services to understand the cyber security implications of emerging and wider technologies