SCOTTISH POLICE AUTHORITY
ÙGHDARRAS POILIS NA H-ALBA

Agenda Item 3.2

Meeting	**Policing Performance Committee**
Date	**18 September 2024**
Location	**Video Conference**
Title of Paper	**Policing in a Digital World Programme Update**
Presented By	**ACC Andrew Freeburn, Organised Crime, Counter Terrorism and Intelligence**
Recommendation to Members	**For Discussion**
Appendix Attached	**Yes – Appendix A: PDWP Annual Report 2024**

PURPOSE

The purpose of this briefing paper is to provide the members of the Scottish Police Authority (SPA) Policing Performance Committee with an update on the progress and direction of the Policing in a Digital World Programme (PDWP).

This paper will specifically provide a progress report in relation to: Agenda item 3.2 – Policing in a Digital World Programme Update

Members are invited to discuss the content of this report.

1. SUMMARY

Introduction

1.1 Policing in a Digital World (PDWP) aims to transform how Police Scotland respond to the evolving threat of cybercrime. The following items detail several of the current projects and workstreams that have progressed since the last update to the Committee.

1.2 PDWP aims to provide the Scottish Police Authority (SPA) with a written update on the progress of objectives every 6 months. To support regular updates, PDWP will prepare an annual report in early 2025 similar to that produced this year (attached as an Appendix A).

Background

1.3 PDWP produced their annual report in March 2024, attached, which highlighted the journey Police Scotland embarked on with the creation of the Cyber Strategy 2020. This acknowledged that Police Scotland had to address the increasing demand from cybercrime, while aligning our approach to organisational strategies and the threat picture while keeping people safe in a digital world.

Now

1.4 In April 2024, four Digital Forensic Triage Vans were successfully delivered to our Digital Forensic Labs. Each van has been meticulously designed to offer a spacious and secure working environment with all the available technology to conduct onsite triage. User feedback, carried out at the conclusion of delivery, has shown increased welfare and comfort, with many appreciating the space and privacy the vans offer. Of the staff surveyed, feedback included "The Cyber Vans have had a significant positive impact on my day to day working environment" and " the van is excellent for working practice and wellbeing". Additionally, the vans' power systems have proven remarkably efficient, with battery usage alone ensuring continuous operation without the need for external power sources. An unmeasured benefit of the vans is recorded as the opportunity for front line officers to also utilise the space, out with crime scenes, to engage with DF officers and improve the ability to discuss investigation considerations.

1.5 In May 2024 the Digital Evidence Detection Dogs project was successfully delivered. Police Scotland currently have 3 dogs, fully deployed nationally and realising the benefits described within the

initial business case. The dogs are improving detections across several business areas to support the investigation of crimes and keeping people safe. As of 27th August 2024, there have been 48 deployments across 11 divisions and 145 device recoveries which include mobile phones, SIM & memory cards, cameras and tablets. Operational Support Division (OSD) are in the process of training another 3 dogs to increase the overall compliment and availability of this resource nationally.

1.6 In August 2024, Police Scotland launched its support to Police Cyber Alarm and will develop and introduce a framework for engaging and supporting local businesses to strengthen their own network resilience. We will also develop proactive engagement activities which will be specific and targeted based on intelligence and developed information as well as improving investigative capabilities and evidential capture opportunities. PDWP will continue to collaborate with Police Scotland Policing Together, Partnerships & Prevention (PTPP), using the Police Cyber Alarm technology to identify and mitigate potential weaknesses and risks, strengthening small and medium enterprise (SME) cyber resilience.

1.7 PDWP produce regular bulletins to our workforce to keep them appraised of programme developments and to seek wider engagement and understanding of programme deliverables. In support of this, PDWP are working with Cybercrime and Digital Forensics to develop the already established Cyber Champions network. Cyber Champions, comprised of officers and staff across Police Scotland, have to date been able to assist investigations with their cyber expertise and promoted cyber related guidance within their local divisions. Building on this, benchmarking with UK LEAs has been undertaken to understand their approach and how such cyber support roles benefit their organisations. Expansion of regular Cyber Champions virtual sessions to over 150 officers/staff including other Police Scotland cyber related cadres, has also been important in developing this role and broadening cyber awareness within the Force.

Next

1.8 PDWP will be supporting several events over the next few months within the wider public sector, to support promotion of Police Cyber Alarm.

1.9 The Cyber Choices Scotland (CCS) project is working towards the development of a Business Justification Case (BJC) with key stakeholder engagement, internally and externally, to support a

strategy that will enhance Police Scotland's preventative approach to identifying and diverting those on the cusp of cyber criminality. Cyber Choices is widely utilised across England and Wales. PDWP continue to link into National Groups to support building the BJC.

Beyond

1.10 In January 2024 ISO 17025 and Digital Forensic Re-Design were combined under one project due to many interdependencies. PDWP have created an updated timeline for ISO 17025 addressing the accreditation deadlines for Aberdeen and resourcing challenges to fulfil our updated commitment. Support to Aberdeen, Inverness and Govan DF Labs in preparation for UKAS assessment is underway. Benchmarking continues against other forces including future resource requirements to support ISO 17025 accreditation.

1.11 The Cyber Training and Capability Project internal training team are now fully staffed until 2025. A workshop was held in August 2024 with key business stakeholders to develop next steps regarding the future approach to the digital training landscape. This included future lifetime management including securing further training lots, internal development, resourcing and investment/funding.

1.12 In September 2024, PDWP hope to begin the governance journey that describes Police Scotland's key requirements needed to enhance its current model to investigate and respond to the threat of Fraud. This is supported with key engagement with City of London Police (CoLP) in relation to the new Fraud and Cybercrime Reporting and Analysis Service (FCCRAS).

1.13 During the scoping and discovery phase for Fraud, aligning our approach to UK LEA's response to Cyber and Fraud, PDWP has uncovered an opportunity to make some internal structural changes to support the Fraud investigation model. This work will be considered under the PDWP Cyber Futures workstream.

1.14 PDWP continues to support the development of the Scottish Cyber Coordination Centre (SC3). SC3 focuses on key areas of incident coordination, cyber exercising and threat intelligence, working with core partners to develop key products that are being shared with the Scottish Public sector and wider. SC3 has just completed a draft of its 3-year strategic plan which is awaiting approval but will provide a roadmap to building on the foundations of the work carried out to date.

1.15 The current capability for mobile phone triage is currently under review with benchmarking taking place with other forces across England and Wales. This will be fully detailed in a new DFRD Business Case by the end of the financial year 2025.

2. FINANCIAL IMPLICATIONS

2.1 We remain in adherence with the agreed budget and associated processes.

2.2 Despite the current organisational financial challenges, in order to meet the ambition of the programme's significant investment in our people, technology, estates, processes and structure is paramount.

3. PERSONNEL IMPLICATIONS

3.1 There are personnel implications associated with this update in terms of the associated projects and deliverables. Longer term, organisational change will be proposed in relation to structures required to enhance capabilities to prevent and deal more effectively with cyber dependant and enabled crimes.

4. LEGAL IMPLICATIONS

4.1 There are no legal implications with the report.

5. REPUTATIONAL IMPLICATIONS

5.1 There may be reputational implications for Police Scotland if the improved capabilities and capacity are not delivered.

6. SOCIAL IMPLICATIONS

6.1 There are no social implications in this report.

7. COMMUNITY IMPACT

7.1 There are no community implications in this report.

8. EQUALITIES IMPLICATIONS

8.1 There are no equality implications in this report. All relevant documents will be completed in line with the formal investment governance process e.g. at Business Case stage. This will include a full consideration and utilisation of the rights-based pathway

alongside relevant EQHRIA and DPIAs being completed where applicable.

9. ENVIRONMENT IMPLICATIONS

9.1 There are no environmental implications in this report.

RECOMMENDATIONS

Members are invited to discuss the content of this report.

Policing in a [Digital World]

Annual Report
2024

Contents

Foreward

Since the launch of our Cyber Strategy 2020, the pace of the cyber landscape and advances in technology has surpassed all our expectations. It is therefore critical that given the threat that cybercrime poses to the people, communities, businesses and assets of Scotland, we must adapt and modernise our policing model, to respond effectively to continue keeping people safe in both the physical and digital world.

Whilst some phenomenal work has already taken place, there is more to do and at pace. The exponential increases in economic crime, ransomware, online fraud, child sexual offending, trading of weapons and trafficking of people on the dark web demonstrates how criminals have become digitally enabled.

As the Senior Responsible Officer for the Policing in a Digital World Programme (PDWP), I am pleased to present the Programmes first Annual Report for 2024.

As an organisation, we are transforming our service on how we respond to the evolving threat of cybercrime, delivering on this commitment, through the investment in our officers and staff, on the frontline and in specialist roles, so that they have the confidence, training, skills, tools and support to meet these new challenges.

In terms of how we pursue cyber-criminality, we recognise the need to enhance our capacity and capabilities and over the last year we have focussed on improving our digital forensics provision, our response to Online Child Sexual Abuse and Exploitation (OCSAE) and Fraud.

As a result, I am delighted to see the introduction of digital evidence detection dogs, trained to detect a wide range of digital devices and digital forensics vans, allowing for ‘at-scene’ examination.

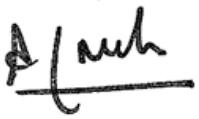
Adding more people to tackle the problem, is not a long-term solution nor a sustainable option. We must continue to explore the new technologies, streamlining processes, making us more efficient and effective whilst having a positive impact on the wellbeing of our people.

The introduction of our Rights Based Pathway meets a joint commitment with the Scottish Police Authority (SPA) to support decision making and to maintain public trust and confidence in the organisation, when adopting the use of technology. I believe that this model is a significant step forward in providing public reassurance – which both keeps people safe, whilst upholding their rights.

Partnerships are key to tackling cybercrime, as we simply cannot arrest our way out of the problem and recognise that there are multiple agencies and organisations who have a footprint in cyber enabled/dependent crime including the response, investigation and intelligence.

There is therefore a need for Police Scotland to continue to collaborate across the entire cyber sector in Scotland, to pull together the collective resources, so that we become more than the sum of our parts.

I would like to take this opportunity to thank the dedicated staff and partners who are working tirelessly to deliver against the priorities of our cyber strategy and our core duty of protecting the people of Scotland.



Andy Freeburn
Assistant Chief Constable
Organised Crime, Counter Terrorism & Intelligence

Policing in Scotland - A Case for Change

POLICE SCOTLAND
Keeping people safe
POILEAS ALBA

Joint Strategy for Policing

Our Vision	Policing for a safe, protected and resilient Scotland
Our Purpose	The purpose of policing is to improve the safety and wellbeing of people, places and communities in Scotland
Our Values	Fairness Integrity Respect Human Rights

Strategic Police Priorities

Crime and Security | Confidence | Sustainability | Partnerships | People | Evidence

Priorities for Policing

Protecting Vulnerable People | Tackling Crime in the Digital Age | Working with Communities | Support for Operational policing

Outcomes	Objectives
Threats to public safety and wellbeing are resolved by a proactive and responsive police service	• Keep people safe in the physical and digital world • Design services jointly to tackle complex public safety and wellbeing challenges • Support policing through proactive prevention
The needs of local communities are addressed through effective service delivery	• Understand our communities and deliver the right mix of services to meet their needs • Support our communities through a blend of local and national expertise • Support the changing nature of communities
The public, communities and partners are engaged, involved and have confidence in policing	• Embed the ethical and privacy considerations that are integral to policing and protection into every aspect of the service • Protect the public and promote wellbeing across Scotland by providing services that are relevant, accessible and effective • Work with local groups and public, third and private sector organisations to support our communities
Our people are supported through a positive working environment, enabling them to serve the public	• Prioritise wellbeing and keep our people safe, well equipped and protected • Support our people to be confident leaders, innovative, active contributors and influencers • Support our people to identify with and demonstrate Police Scotland values and have a strong sense of belonging
Policing is sustainable, adaptable and prepared for future challenges	• Use innovative approaches to accelerate our capacity and capability for effective service delivery • Commit to making a positive impact through outstanding environmental sustainability • Support operational policing through the appropriate digital tools and delivery of best value

Performance and Implementation

Evidence led policing

Strategic Context

Police Scotland has made a commitment to 'keep people safe in the physical and digital world', with 'Tackling Crime in a Digital Age' a priority. The Cyber Strategy 2020 supports this, and we should ensure that our work aligns with the key deliverables and outcomes.

Strategic Threat & Risk Assessment (STRA) 2023/28

The recently published Strategic Threat and Risk Assessment (STRA) highlights that one of the biggest growing operational demands on Police Scotland is cybercrime. This area has rapidly evolved, with reports more than doubling over the last 6 years and with traditional crimes now having a digital footprint.

The demand on Cyber Investigations alone to support operational Officers with their investigations in relation to cryptocurrency investigations has risen by 1150% in under two years. This highlights a gap in knowledge that frontline officers need to investigate cybercrime effectively and with confidence in their ability to do so.

Cyber enabled and cyber dependent crime has been increasing for a considerable period of time and this has escalated further during the COVID-19 pandemic. Having no geographical boundaries, cybercrime as a whole affects local and wider communities and businesses by exploiting advances in digital technology and vulnerabilities of victims.

This is an area of increasing risk and Police Scotland must ensure that its policing model can respond effectively.

Alignment to UK Cyber Strategy

It has been decided to align the objectives of the Police Scotland Cyber Strategy to that of the UK Government National Cyber Strategy 2022. This ensures that as a public sector body are working in line with wider national government outcomes.

Violence Against Women and Girls Strategy (VAWG)

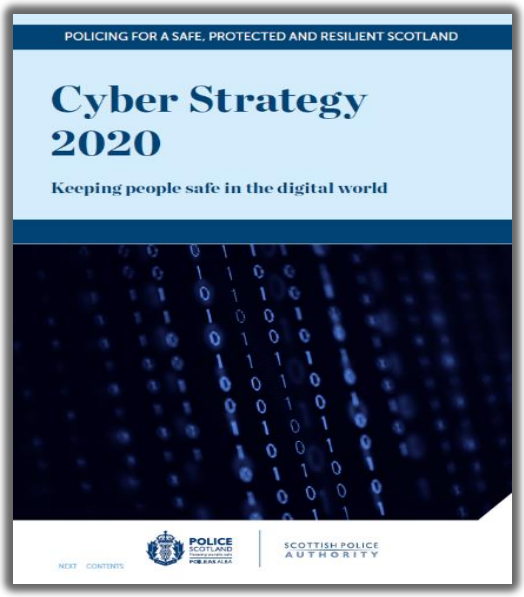
Our Violence Against Women and Girls (VAWG) Strategy also outlines how Police Scotland aim to protect women and girls from crime executed through digital spaces. It highlights that Police Scotland is committed to disrupting perpetrators and preventing harm wherever it takes place. We recognise the specific threat cybercrimes present and are working to adapt our services to keep people safe online. It leans on the cyber strategy to help develop the organisational capability and capacity to proactively identify and investigate threats.

The VAWG Strategy states that to meet future demand we will direct our resources to deliver an effective, pro-active, intelligence-led service which identifies perpetrators and protects those at greatest risk of harm.

As VAWG explores, the manipulation of technology and social media poses a risk for both adults and children, with women and girls disproportionality affected. The pace of technological change, and the constant evolution of tactics deployed by perpetrators, means policing and other criminal justice system partners must be equipped with resources to disrupt these threats and protect people from harm.

Of particular concern is the rise in OCSAE. This type of offending includes the taking, distribution or viewing of indecent images of children, online grooming, inciting children to commit sexual acts online and live streaming of sexual abuse.

Police Scotland Cyber Strategy – The Journey So Far



The Police Scotland Cyber Strategy 'Keeping People Safe in the Digital World' was approved by the SPA Board on 30 September 2020. The ambition of the strategy was to bring about the comprehensive change necessary to become a centre of excellence in digital and cyber policing.

The Policing in a Digital World Programme (PDWP) was formed with the clear aim to transform how Police Scotland respond to the evolving threat of cybercrime.

The Programme has embedded a 4P's approach to dealing with cyber related threats (Pursue, Protect, Prepare and Prevent), in line with the National Police Chief's Council (NPCC) led 'Team Cyber UK' methodology.

By ensuring all officers and staff on the frontline and in specialist roles have the knowledge, skills, tools, and support to confidently and effectively tackle cybercrime, Police Scotland will be better equipped to prevent, respond to, and investigate such crimes; we must build the workforce and tools to keep people safe in public, private and virtual spaces.

This enables Police Scotland to:

- Focus on an improved victim experience (overarching outcome).
- Deliver an effective investigative response (Pursue).
- Target local cybercrime prevention messaging (Protect).
- Work to identify and divert people vulnerable to engaging in cybercrime (Prevent).
- Engage with businesses and organisations to help them develop effective measures to mitigate threats and risks associated with cybercrime and, where appropriate, engage in testing and exercising (Protect).
- Develop Centres of Excellence and provide guidance to the wider force, helping mainstream cyber skills and knowledge into most areas of policing (4P approach).

Professional Services

PricewaterhouseCooper (PwC) and PDWP reviewed Police Scotland's current cyber capabilities, whilst benchmarking against UK and international standards. This helped develop the following:

- Critical Friend Review of the Cyber Strategy
- Cyber Target Operating Model
- Capability Assessment
- Presentation Products
- Strategic Outline Business Case

Using a capability model, PwC produced a high level Target Operating Model (TOM) and a costed Strategic Outline Business Case (SOBC).

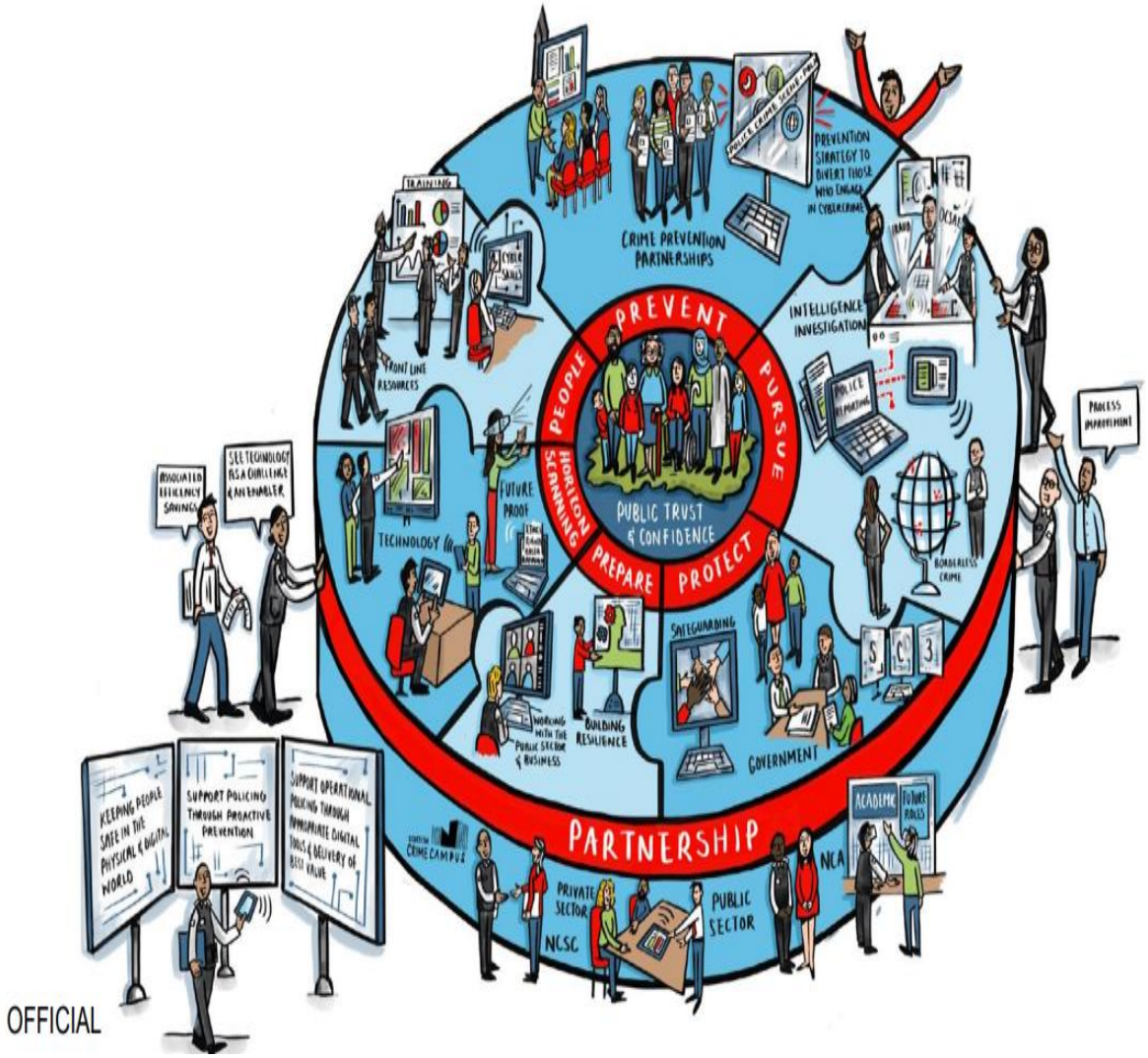
This journey allowed for the formulation and adaptation of the objectives focussing on the traditional 4P approach of Pursue, Prevent, Protect and Prepare methodology, with the additional key

overarching components of People, Partnerships and Horizon Scanning.

The evolution of this approach was to create more holistic and sustainable model for developing Police Scotland's Cyber Capabilities and preparedness for future threats.

With public trust and confidence at heart, the diagram below, depicts the 'pieces of the jigsaw' required to brings about a whole system approach to tackling the problem.

The report expands on each of these areas and outlines the work being undertaken in achieving or contributing to the objectives of the strategy and linked strategic outcomes.

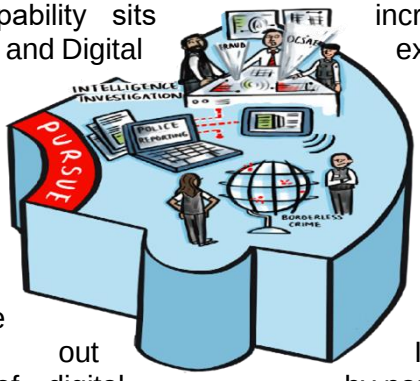


Pursue

This focuses on our ability to pursue individuals, groups and larger organisations involved in the most serious cyber threats to Scotland by prosecuting and disrupting cybercrime. Through collaboration and critically analysing the threats facing Scotland, PDWP understand the need to collaborate with national and international law enforcement, to provide a multi-disciplinary approach to tackling cyber. Within this work was an identified need to provide new capabilities to our investigation and intelligence teams which would enhance our ability to investigate cyber related offences.

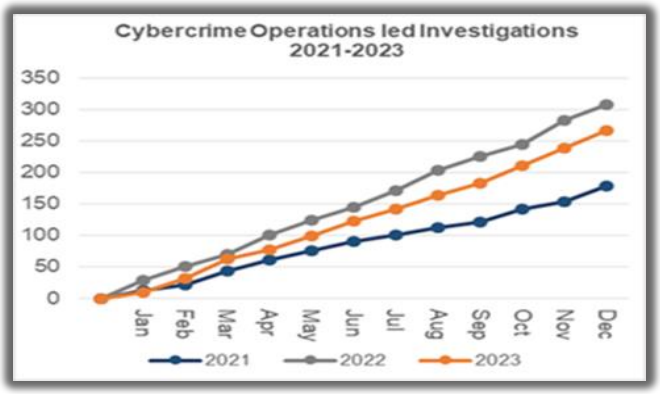
Police Cybercrime Investigations and Digital Forensics

Police Scotland's Pursue capability sits within Cybercrime Investigations and Digital Forensics (DF). Cybercrime Investigations are responsible for providing specialist support and undertaking investigations into high-end cyber-dependant crimes.



Digital Forensic Units are responsible for carrying out examinations and analysis of digital devices and CCTV as well as providing expert advice, specialist recovery services and reports for court.

Between 2016 and 2022, the Investigation team have seen a 2000% (16-220) increase in cyber related crimes.



Also given the digital footprint on everyday life, this has had a direct correlation with the increased demand in digital forensic examination requests that cuts across local and specialist policing, with 3982 requests containing 16,771 productions being processed in 2023.

This is exacerbated by even more Internet Enabled Devices (often referred to as the Internet of Things - IoT) with the capability to be utilised by nominals to commit crimes.

Further, the data storage capacities and security protocols which are now innate to these devices as well as their associated applications and internet enabled services are both far greater than at any point in this past.

Developments and improvements in this area aligns to the priorities of the PDWP and the associated projects and work streams that are outlined in this report.

STRA Recommendation: Ensure the Sustainability of Digital Forensics hubs to meet increasing demands over the next five years and reverse Capacity and Capability deficits as outlined in the Digital Forensics Workforce Review of March 2022.

ISO 17025 Accreditation Project

In 2019, a short life working group (SLWG) was established by the Scottish Police Authority (SPA) to review digital forensics within Police Scotland.

The SLWG identified ISO 17025 as the most appropriate quality standard for adoption of DF laboratory work, and once accredited, Police Scotland should voluntarily adhere to the Forensic Science Regulators Codes of Conduct and Practice as mandated for England and Wales.

Now

Police Scotland's has five Digital Forensics (DF) laboratories, each of which will require to be assessed by the United Kingdom Accreditation Service (UKAS) against the ISO/IEC 17025:2017 Standards.

The first of these laboratories is the Aberdeen site for which the application to UKAS is complete. The UKAS assessment requires policies and procedures to address and comply with the standards set out in ISO/IEC 17025:2017.

Aberdeen DF is now operating in to these policies and procedures awaiting assessment for mobile phone extraction and examination

Next

Over the coming months Aberdeen DF will continue in preparation of the UKAS assessment which is anticipated to take place around June – July 2024.

Meanwhile preparations will progress for the second DF laboratory that will be subject to accreditation – the Inverness site, including site visits from the ISO 17025 Project Team as well the UKAS application process.

Beyond

Following the assessment by UKAS at the Aberdeen DF site feedback and any remedial action undertaken based upon feedback. It is anticipated formal accreditation for Aberdeen will be around September – November 2024.

Digital Forensics Re-Design Project

Digital Forensics is a specialist function of Police Scotland that assists in the examination and analysis of digital evidence on phones, computers, tablets and other multimedia.

Extensive analysis has identified that investment and development of the business area is required to meet demand and exploit available tools and technologies while attracting the right people with the right skills into the organisation.

Now

Police Scotland's DF Laboratories require investment to enhance their capabilities to create efficiencies and keep up with the continual technological developments which the public and criminals have access to and utilise on a daily basis.

Work is underway to consider recommendations made across 5 key themes which affect DF namely People, Wellbeing, Estate, Technology and Processes. This is with a view of creating a future operating model to meet demand and equip our staff with the right tools to undertake their demanding role.

Next

The priority for FY24/25 will be process and technology. Given the current financial and resource picture within Police Scotland, PDWP are working to ensure that Digital Forensics has current technology and processes in place to create efficiencies where applicable, and to minimise delays in the Criminal Justice process and enable our staff.

Beyond

The Chief Constable's aspiration is for "Police Scotland to be the most digitally enabled police force in Europe, using technical capabilities to improve both our efficiency and effectiveness." PDWP will look to enable Digital Forensics to meet demand, improve officer wellbeing and in turn will providing a better service to stakeholders and members of the public.

Digital Evidence Detection Dogs

Police Scotland recognises that officers and staff are under continued pressure to investigate ever increasing numbers of crimes which have a cyber or digital element.

In order to keep up with technological advances, evolving criminality, the PDWP in conjunction with our Operational Support Division (OSD) will introduce the new specialism of Digital Evidence Detection Dogs.

The organisation currently relies upon human search techniques (conventional and specially trained officers) to locate and identify digital devices which may be relevant to an investigation. Current advances in technology and criminal behaviour mean the detection rate for cyber and digital crime remains low.

6 Digital Evidence Detection Dogs with 3 dedicated handlers are initially being introduced to provide a national capability which up until now has been facilitated through the provision of Mutual Aid. Training dependent, the provision will be operational in Spring 2024 and an associated communication plan is in place.

Once operationally deployed, an evaluation will be carried out, with the associated benchmarking indicating that this will likely result in justification to increasing the provision of dogs and handlers, which is in keeping with the rise of cyber related crimes.

Digital Forensic Vans

Victims, witnesses and suspects may experience periods of time where they are deprived of their digital devices if they are seized for examination as part of a criminal investigation.

Police Scotland currently have limited options in terms of examining digital devices seized under legislative powers or by agreement of the owner out with Digital Forensics Laboratories.

Any options currently available are sub-optimal and do not always provide suitable or safe working environments for our staff. Existing processes do not maximise efficiencies or reduce the number of devices requiring to be seized for further examination.

The provision of Digital Forensics Vans within Police Scotland will maximise efficiencies and provide a suitable and safe working environment to our officers and staff and provide a better service to the people and communities of Scotland.

Examination of digital devices at the earliest opportunity provides the optimum prospects of identifying investigative lines of enquiry and also reduces the delay in the device owner being deprived of this for extended periods for examination.

CAID/Online Child Sexual Abuse and Exploitation

CAID is the Child Abuse Image Database and contributes to the fight against Online Child Sexual Abuse and Exploitation (OCSAE). It is led by the Home Office.

It helps identify and safeguard victims, makes investigating Child Sexual Exploitation and Abuse faster and more effective and supports international effort to remove images from the internet.

Police Scotland has contributed to CAID since 2015 and continues to engage with the Home Office in the fight against OCSAE using the current tools available. In June 2023, Police Scotland introduced CAID Facial Matching to enhance our current use in tackling the threat

February 2024 – As part of the continuous improvement of CAID, the use of CAID Image Classifier and Cyacomb "at scene" triage tool have been approved for use.

We will continue to work closely with the Home Office in terms of improvements to CAID, whilst developing relationships with UK and International partners to in tackle the global threat of Online Child Sexual Abuse and Exploitation (OCSAE) while improving the wellbeing of our officers and staff.

Cyber Kiosks Phase 2

In 2019 Police Scotland introduced 41 purpose-built standalone digital triage devices (Cyber Kiosks) across the country to enable trained officers to review data stored on digital devices and SIM cards without the requirement to submit the device to a Digital Forensic Laboratory.

Now
The 41 Cyber Kiosks are standalone terminals and require digital forensics staff to attend at the locations in person on a regular basis in order to install software updates, carry out maintenance, repairs and collect management information in respect the use.

Next
PDWP are working in conjunction with Digital Division to find a solution to create a closed network for the Cyber Kiosks to allow for the remote distribution of software updates and remote collection of the management Information. This will bring about efficiencies in terms of negating the current travel time, allowing staff to focus on their core function. It will not share evidence or information from any seized devices.

Beyond
Consideration will be given as to how Police Scotland could enhance the capability of the Cyber Kiosks to provide evidential material at a Cyber Kiosk and prevent duplication of work and in turn create efficiencies and speed up the Criminal Justice process.

Dark Web

Whilst most cybercrime occurs via the surface web, or what would generally be described as the internet, there is another part of the internet, known as the dark web, which is increasingly used to commit crime, often on an industrial scale.

The dark web is not visible to search engines like Google and is accessed through an anonymising browser called the onion router (Tor).

As a result, the dark web has become easily accessible for today's criminals to arrange the supply of commodities (e.g. controlled drugs, counterfeits, firearms, data), commit acts associated to human trafficking and be a method for committing facilitate other cybercrime, such as extortion, fraud, ransomware attacks and livestreaming of sexual abuse.

Police Scotland's Cyber Strategy outlines our priority to increase the organisation's dark web presence and investigative ability. This will enable us to pro-actively deploy specialists to enable a greater assessment and understanding of the threat to our communities

Now

Police Scotland currently form part of TeamCyber UK and as part of this work closely with the NCA in terms of their Darkweb Intelligence Collection and Exploitation Unit (DICE) and Regional Darkweb Operations Teams (RDOTs) who are based within each of the 9 Regional Organised Crime Units along with the Met Police, under the leadership of the Regional Cybercrime Units.

Next

PDWP are engaging with the associated business areas with a view to introducing a dark web capability into the organisation whilst exploring becoming part of the established UK Dark Web network.

Beyond

By increasing our capability and by training and equipping our people, will better enable us to form part of the global network of law enforcement specialists that can work together to share knowledge and tactics to tackle dark web criminality effectively, with increased ability to unlock evidence on encrypted devices and networks.

Cryptocurrency

Since 2019, Police Scotland has experienced a 1900% increase in cryptocurrency related criminality.

As technology evolves serious and organised crime groups are quick to adapt and utilise new methods to help obfuscate their activities with the use of cryptocurrency being one such method.

Police Scotland currently have a limited cryptocurrency capability compared to other UK forces and the Regional Organised Crime Units (ROCU's) who have both and proactive and reactive model.

This is enabled through joint Home Office funding in relation to the investigation of cryptocurrency, procured through the NPCC and for which Police Scotland does not benefit from. This included a recent award of £1.5 million over 2 years.

Through Scottish Government, Police Scotland is currently exploring funding opportunities to procure licences to support the tracking and investigation of cryptocurrency.

The licences will ensure Police Scotland have the capacity, skills and knowledge which allows the organisation to keep pace with that of UK and global Law Enforcement Agencies and partners to then maximise the opportunities to disrupt, enforce and prevent digital assets from funding SOCG activities.

An increased Intelligence capability allows for targeted and focussed activities towards disruption and also preventative and protection measures being deployed.

Critical Issues

The Critical Issues Project sought to address the issues associated with the internet Investigations Unit (IIU) database used to record, manage and track volume OCSAE referrals.

With the "critical issue" now having been addressed through the Data Drives Digital Programme, the project has been approved for closure.

The PDWP and the Chief Data Office are now exploring the opportuntiies with regards to the introduction of a single search and text analytics capability by the organisation.

Protect and Prepare

Protect *focuses on the support we provide businesses, organisations and the public from cybercrime. We identified that working in conjunction with partners to better identify and safeguard the most vulnerable members of society from cybercrime; continually drawing on cutting edge technologies to protect the most vulnerable in our communities.*

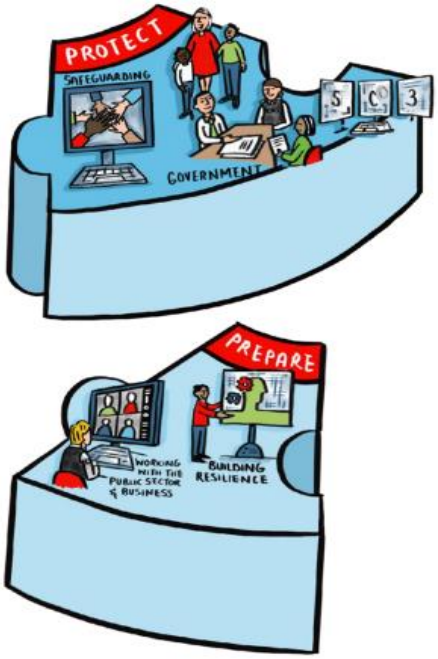
Prepare *requires us to be impactful and deliver world-class training and engagement with the public and business to more effectively build resilience within the community to reduce victimisation.*

Partnerships, Prevention and Community Wellbeing (PPCW)

Partnerships, Prevention and Community Wellbeing Division (PPCW) provides focus on primary prevention using the skills and contributions of partners to deliver guidance and advice to other business areas. The overarching aim of PPCW is to improve the safety and wellbeing of individuals, localities and communities in Scotland.

This can only be achieved through a whole system approach, to tackle the complexities and issues faced by those most in need of our services.

PDWP are working closely with PPCW to develop a Cybercrime Harm Prevention Plan in support of the overall strategy. There will be a focus on a public health approach to reducing cybercrime and will ensure that partners from a range of sectors can positively influence and support our objectives.



A Police Scotland Cyber Prevent Target Operating Model will be explored.

Cyber Harm Prevention

The Cyber Harm Prevention (CHP) Team are located across the North, East and West of Scotland. CHP work closely with the NCSC (National Cyber Security Centre) along with our partners in the public, private and third sectors to deliver cybercrime prevention advice.

CHP liaise with the Scottish Government Cyber Resilience Unit, National Cyber Protect and Prevent networks and Regional Organised Crime Unit (ROCUs) to share best practice, develop our understanding of emerging cyber threats, and trends to provide the most up to date information. They also work closely with the NCA (National Crime Agency) to deliver the national Cyber Choices Programme which helps young people make informed choices and to use their cyber skills in a legal way.

Internal awareness within Police Scotland is an important role of a Protect Officer role by supporting the curriculum of the CTSA offshore Security Awareness Course as well as upskilling officers attending training at the SPC.

Case Study

Police Scotland recently supported a Scottish University following a Protect situation.

The Protect Officers were deployed to support the organisation through the recovery phase after a cyber-attack.

By engaging the leadership team at an early stage to assess their needs, the officers created bespoke guidance in relation to good cyber hygiene, which could be shared with those affected by the attack.

As part of the support package, officers recorded a webinar which was uploaded onto their internal intranet site maximising reach.

Protect Officers work tirelessly to ensure that businesses and organisations, across Scotland, are able to plan, prepare for, respond to, recover and warn from, a cyber-attack.

Police Cyber Alarm

The Police Cyber Alarm (PCA) began as part of the NPCC Cybercrime Programme with initial testing and proof of concept trials being undertaken in 2018 across four regions in England. Although this was an NPCC tool, it was specifically developed as a product for the Small & Medium Enterprises (SME) to use to inform and advise on areas of potential vulnerability within network infrastructures to allow mitigation and protection measures to be put in place.

The Police Cyber Alarm Project, as part of PDWP, will develop and introduce a framework for engaging and supporting local businesses to strengthen their own network resilience, develop proactive engagement activities which will be specific and targeted based on intelligence and developed information as well as improving investigative capabilities and evidential capture opportunities.

Now

After a significant period of discovery and analysis, PDWP are currently progressing a business case through internal change governance for approval in February/March 2024.

Alongside this we are collaborating with Police Scotland's Cyber Harm Prevention Team and the Cyber Scotland Partnership to identify SME's to form part of the PCA launch.

Next

PDWP are working towards a launch of the PCA in Spring 2024 and this will see an initial number of SME's using the technology to receive vulnerability reports and available scanning to identify and mitigate potential weaknesses and risks.

Beyond

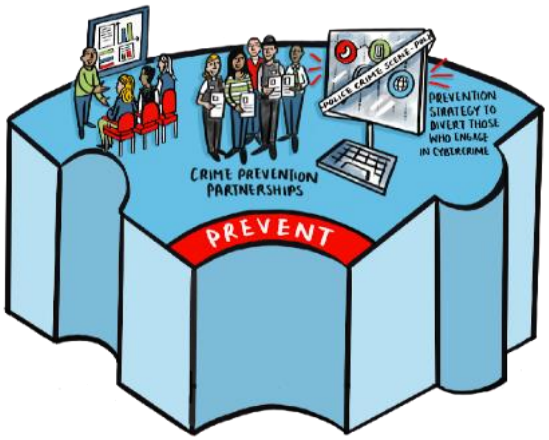
The future picture for PCA is to become embedded within Police Scotland's Cyber Prevent, Protect and Pursue strategies in identifying potential weaknesses and vulnerabilities and mitigating these to strengthen SME cyber resilience.

Police Scotland will utilise potential opportunities to identify those on the cusp of cyber criminality and divert them onto more positive pathways and through analysing increased cyber intelligence benefits and opportunities will be seen and acted upon across the Scottish cyber landscape.

Prevent

It is Police Scotland's ambition to develop a world-class Prevent capability, where we draw on our enhanced intelligence picture to better identify potential perpetrators of cybercrime, and work with partners to better divert individuals from crime, eliminating the pathways to criminality and reducing the impact and harm to society.

Throughout UK Law Enforcement, we recognise that there is a significant lack of public awareness of offending in terms of the Computer Misuse Act 1990 which can result in young people inadvertently straying from curiosity to offending. We have a duty to preventatively educate and safeguard our communities from personal exploitation in the digital world.



The Cybercrime Harm Prevention (CHP) Team has recently started engaging with partners including Education (Scotland) regarding Prevent activity and the Cyber Choices Scotland programme which aims to raise awareness of the risks of venturing into Computer Misuse Act offending behaviour and diverting them towards using their cyber skills ethically and within the boundaries of the law.

Cyber Choices Scotland

Cybercrime attracts young offenders, and with the skill barrier to entry into cyber criminality lower than it has ever been. Off the shelf hacking tools, which require very limited technical expertise to utilise, are available at little to no cost for the user. Many illegal products are advertised openly on low level hacking or gaming forums. Video guides and step by step tutorials on how to use these products are readily available.

In the National Crime Agency's (NCA) National Cyber Prevent Network Delivery Strategy 2018-2020, they highlight concerns about the potential numbers of young people becoming involved in cybercrime. Whatever the motivations are, it is also recognised that a high proportion of those who become involved are either young, vulnerable or neurodivergent.

Now

PDWP have undertaken extensive engagement and workshops involving both internal and external stakeholders and organisations to recognise the gap in identifying, engaging and diverting those on the cusp of cyber criminality. This initial work has already established a collaborative approach through the Cyber Choices programme in which this will be adopted for delivery in Scotland through Cyber Choices Scotland.

Work continues across the organisation in benchmarking and engaging with partners to deliver a bespoke and meaningful delivery package of intervention and diversionary options. Recognition of cyber behaviour as a stand-alone risk and harm has resulted in a specific Cyber Risk tag being added to the organisations risk and concern reporting process which allows for cyber specific harms to be identified and managed through our concern hubs in collaboration with our Cyber Harm Prevention Team.

Next

PDWP will progress the Cyber Choices Scotland Project through governance and continue to work with UK partners to deliver a framework for Scotland.

This work includes cyber specific risk assessments tools, supported sign off programme, training and also Scottish based intervention delivery options through a delivery partner.

Beyond

PDWP will deliver Cyber Choices Scotland through governance with a launch date during Summer/Autumn 2024 to coincide with the new school term.

PDWP will also deliver as part of a phased implementation a Cyber Choices Scotland disposal framework allowing for those within the youth justice system to be signposted and diverted onto a suitable intervention programme as an alternative to youth justice and criminal proceedings.

Case Study

In 2023 Collaboration within Academia supports the foundations of Prevent, in particular engagement with Abertay University's Cyber Quarter.

Abertay University helped promote careers in Cyber by providing an opportunity for CHP to talk to 150 female school pupils about the Computer Misuse Act 1990 and ethical hacking.

Case Study

In 2023, CHP worked with Smart STEMS, (a 3rd sector organisation with aims to raise awareness of Science Technology Engineering and Maths (STEM) careers amongst children) which has provided the team opportunities to reach key audiences including neurodivergent and socioeconomically deprived school pupils.

To date have we delivered workshops and engagements at over 25 events across Scotland to over 5,000 young people in primary and higher education.

Case Study

In 2023, as part of our Cyber Choices Scotland programme the CHP Team has been engaging with young people who have skills and a keen interest in cyber and have developed Cyber Careers Week.

This is a virtual work experience programme which has been developed to up to thirty S4-S6 pupils at a time throughout Scotland. Attendees receive over 25 hours of content and participate in activities including developing their understanding of Open Source Intelligence (OSINT), social engineering, the ransomware kill chain and the CHP team's role in response to cyber-attacks.

The students are tasked with developing their own response to a ransomware attack including elements of information sharing protocols, media strategies and the importance of exercising to prepare for potential attack.

People

PDWP recognises that a workforce of the future comprises a blend of police officers and police staff, who are all digitally aware and continuously skilled to better deliver against the criminal of tomorrow. Attracting the best graduates from top Scottish universities and creating career pathways that excite will help us retain talent. In order to achieve this, PDWP recognised that the undernoted points would be key to underpinning a sustainable model to future proof our people.

STRA Recommendation: Strengthen Police Scotland's commitment to tackling crime in a digital world by developing our investigative capacity and capability regarding cyber enabled fraud which continues to target the most vulnerable in our communities.

It is ambition of the PDWP to deliver a workforce of the future that comprises a blend of police officers and staff, who are digitally aware and continuously skilled to better deliver impacts against the criminal of tomorrow.

This also includes the need to diversifying the role of special constables and volunteers whilst attracting the best graduates from top universities with career pathways that excite and retain talent.

The key to achieving this is by ensuring that our people are equipped with the right tools, training and technology to carry out their roles, to help deliver the best possible service to the public.

Cybercrime First Responder Guide

The Cybercrime First Responder Guide was created to provide police personnel at all levels with the skills and information required to investigate cybercrime. It has been refreshed by PDWP and has been updated to reflect both Scottish Legislation and current Cybercrime investigation techniques.

PDWP are currently exploring the additional training needs/requirements of people through the Cyber Training and Capability Project.

Cyber Training and Capability Project

The Cyber Training and Capability project seeks to enable Police Scotland's officers and staff with the capability and capacity to respond to threats and establish ways to prevent, protect and pursue to the ever more inventive and complex use of digital tools and tactics.

The training will be delivered across 3 levels:

Foundation: Frontline Officers and staff including investigators who are the first point of contact or first to arrive at the scene or locus, and those identifying opportunities that may exist around digital and cyber enabled crime.

Intermediate: Staff and Officers who have the skills in addition to their main role in division to investigate digital/cyber enabled/ dependent crimes. Those who have a general understanding and appreciation of cyber enabled/dependent crimes and the investigative opportunities they present.

Advanced: Staff and Officers who are in specialist roles which predominately investigate digital/cyber enabled/ dependent crimes. Those who are competent in cyber digital investigation and have a sound understanding and appreciation of cyber enabled/dependent crimes and the investigative opportunities they present.

Following Initial Business Case approval by the SPA Resources Committee in May 2023, the following preferred option was supported to progress to Full Business Case development:

"Develop a globally recognised, adaptive and forward looking cyber and digital training structure through a hybrid delivery model. Internal capability is significantly enhanced and skills gaps are eliminated through development and dissemination of specialist training packages, optimising relationships with partners."

In July 2023 an open procurement process commenced covering 8 distinct lots:

1. Foundation (Gamified Learning Platform)
2. Cryptocurrency Intermediate
3. Dark Web Intermediate & Advanced
4. Economic Crime Intermediate
5. Ethical Hacking Advanced
6. Incident Handling Intermediate & Advanced
7. Malware Advanced
8. Neurodiversity Intermediate

This process is still ongoing and when concluded, the outcome of this process will be communicated in line with Police Scotland's Investment Governance Framework.

Work is ongoing in respect of the creation of a dedicated cyber training space at the Scottish Police College alongside the recruitment of a Cyber & Digital training team, who will design and deliver the range of cyber courses.

Partnerships

Partnership working and a Multi-Agency response to combating cybercrimes draws on a whole system approach. Police Scotland have a clear view of their roles and responsibilities, and other partners take the lead on areas they are better equipped to.

To successfully tackle the threat posed by cybercrime requires collaboration between the public and private sector and there is a genuine appetite off all to enhance relationships given the scale. By working in partnership across different organisations and sectors, we can bolster our ability to combat cyber threats.

PDWP have identified and developed strong working relationships with a number of organisations across the Cyber landscape in terms of law enforcement, public, private, and third sector partners. In harnessing these close working partnerships, Police Scotland is looking for ways to work more collaboratively and seamlessly together, whilst breaking down any remaining divisions that may exist across the public, private and the voluntary sector.

Cyber Scotland Partnership

The Cyber Scotland Partnership is a collaboration of key strategic stakeholders, brought together to focus efforts on improving cyber resilience across Scotland. It represents a commitment from partners to work together to drive the delivery of activities that will help achieve the outcomes of the Strategic Framework for a Cyber Resilient Scotland.

Partners work collaboratively to:

- build Scotland-wide cyber resilience
- increase effectiveness and impact, avoiding duplication of effort
- improve communication and knowledge-sharing relating to cyber threats
- provide a single online portal for organisations, businesses and individuals seeking information, guidance and support on cyber resilience issues (cyberscotland.com)
- promote national events, in particular the annual Cyber Scotland Week
- collectively support the cyber security community

Police Scotland are an active participant in this partnership supporting activity through the year with a focus on the objectives mentioned above.

Cyber and Fraud Centre (Scotland)

A key member within the Cyber Scotland Partnership is the Cyber and Fraud Centre (Scotland). Their vision is to make Scotland one of the safest and most resilient places to live, work and run a business. They offer a range of services and guidance to people and businesses in the Prevent/Protect categories while educating and training those to become more resilient and better prepared to mitigate future cyber threats.

They were also instrumental in the creation of the aforementioned Multi-Agency Fraud Triage Hub (page 27).

Scottish Cyber Coordination Centre (SC3)

The Scottish Cyber Co-ordination Centre (SC3) has been created in conjunction with Scottish Government and senior representatives from across the public sector within Scotland. SC3 aims to develop a more collaborative approach which would support more effective intelligence sharing, assessment of national cyber threats and risk, testing and exercising and incident response/recovery.

Police Scotland are a core partner of SC3, and with other closely aligned Public sector bodies, is contributing to shaping the role for SC3 in Scotland whilst maximising the opportunity to collaborate in the fight against the cyber threat. SC3 now publishes threat intelligence reports daily to the public sector and shares this content via the Cyber Scotland Partnership website.

Throughout early 2024, SC3 hope to support Cyber Exercising and Training, and Incident response and Vulnerability. Both these areas are of importance and relevance to Police Scotland who will support developments in these areas to better inform and prepare Police Scotland to deal with the Cyber threats facing Scotland and protect its communities.

PDWP Professional Reference Group

Police Scotland and the SPA's joint vision is to deliver comprehensive change to become a centre of excellence in digital and cyber policing. Following publication of the Cyber Strategy, the focus has been on planning for implementation and engagement with stakeholders and the public.

The SPA is committed to supporting Police Scotland in building public trust through open and transparent discussion and engagement, promoting and supporting the need to build effective preventative partnerships and secure additional investment.

It is recognised that the strategy, implementation and engagement plan will benefit from collaboration with key industry and public partners led by both Police Scotland and the SPA.

This will support strategic delivery, while offering informed expertise and effective challenge as Police Scotland progresses with implementation of this future focused strategy.

This resulted in the creation of the joint (SPA and Police Scotland) PDWP Professional Reference Group (PRG) with the inaugural meeting taking place on 22 September 2002.

The PRG is chaired by DCC Jane Connors Graham and SPA Board Member Caroline Stuart, with representation from the National Cyber Resilience Advisory Board, Cyber and Fraud Centre (Scotland), Academia and the Equality and Human Rights Commission.

In the last meeting, which took place in January 2024, the group specifically explored the risks and opportunities on the police use of Artificial Intelligence and how Police Scotland could more effectively communicate and engage with the public on the introduction of new technologies.

Academia - Abertay cyberQuarter

The PDWP following initial approval are currently exploring becoming a member of the Abertay cyberQuarter**.**

The £18m hub was opened in June 2022 within Abertay University, Dundee having been jointly funded by the University, UK Government and Scottish Government, through the Tay Cities Region Deal, providing a new model for supporting the rapidly growing cyber sector in a facility that's the first of its kind in the country.

The initiative brings together students, academics and organisations to help solve global cybersecurity challenges. Following engagement, the key benefits and collaboration opportunities in addition to consultancy include:

- Research and Development (R&D) - Access to specialist resources, technology and infrastructure.
- Knowledge Transfer Partnership - Projects to address specific strategic challenges, where together new knowledge/expertise is created.

Communication and Engagement

Recognising the need to enhance and adopt an effective communications and engagement plan in support of the Cyber Strategy. A communications plan across all cyber activity is being reviewed and developed around the capabilities discussed in this report.

In terms of public engagement, Police Scotland will have one co-ordinated programme of engagement which captures all current and developing approaches under one plan going forwards.

Police Scotland welcome their latest recruit: SIM-card sniffer dogs

Six spaniels are joining the ranks to detect the scent of electronic storage devices used by paedophiles and sex traffickers

This ensures a cohesive, coherent conversation with the public and stakeholders. Design, development and oversight of all elements of public engagement will sit within Strategy and Analysis to ensure that all areas of Police Scotland are supported and that all activity aligns to the agreed approach and themes.

A key theme within the engagement approach is 'Policing in a Digital World', which stretches beyond emerging technology to capture views on broader questions reflected in our strategies, such as Cyber.

This will include exploring areas such as the visibility of policing in the physical and virtual world; the role of policing in online crime; the use of technology enabled policing tools.

Over the course of 2023, Police Scotland attended a number of public sector events to discuss our journey, in pursuit of the objectives discussed throughout this report.

In February 2023, CS Conrad Trickett provided a key note speech at the Future Scotland Event during Cyber Scotland Week in terms of how Police Scotland defend against, and be resilient to, the threat of cyber. This event was attended by public, private and wider members of the community of Scotland who were present to learn how we can all contribute to the cyber security posture of Scotland. Collaboration was the key messaging and the many forms that contribute to this.

In October 2023, ACC Andy Freeburn presented at the Cyber Scotland Summit in Edinburgh again where he took the opportunity to outline our Pursue/Prevent activity, whilst reinforcing the importance of partnerships that are echoed throughout this this report.

The ACC has also facilitated a number of media interviews with regards to the current escalating risk posed by cyber and fraud, the human impact and the organisations response.

Police face cyber crime epidemic

As cases double each year with 50 victims a day, top cop sets his sights on crushing the cruel web crooks

By Ashlie McAnally

CYBERCRIME in Scotland is doubling each year as criminals use technology to dupe unsuspecting victims out of millions of pounds.

In a world where business, socialising and com-

frauds are committed each year in Scotland – or around 50 each day – and according to our own figures 95 per cent of all frauds have an online element and it is now synonymous with cybercrime.

"Behind every one of these frauds

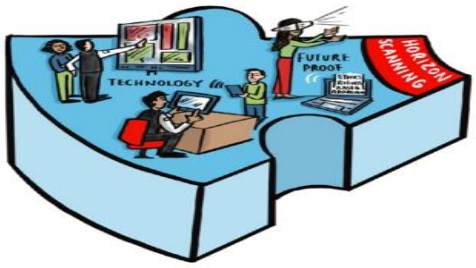
Horizon Scanning

PDWP believe that a police service that is adaptive and responsive: future proofed to stay abreast and ahead of the changing threat, technological, strategic and environmental landscapes.

STRA Recommendation: Strengthen Police Scotland's commitment to tackling crime in a digital world by developing our investigative capacity and capability regarding cyber enabled fraud which continues to target the most vulnerable in our communities

Police Scotland's Strategic Approach to Tackling Fraud

Fraud is a significant global issue which is recognised as the most prominent crime type within the UK, with national reporting of frauds in its' many guises rising whilst detection rates are falling. A previous Scottish Crime and Justice Survey (SCJS) and other insights continue to tell us that the public are deeply concerned about the risk posed by fraud.



Police Scotland's recorded fraud crime reports have increased by 87% in the past 5 years with our detection rate falling by 19% over the same period. Additionally, 95% of fraud is now online and it has become synonymous with cybercrime.

In 2022/23 the force recorded 16,879 fraud crime reports (an average of 46 per day), which is an increase of 8% on the previous year. The total number of detected crime reports over the same period equated to 2,725 (16.1%). It is also believed that this crime is hugely under-reported.

Behind these crime reports are individual victims who have lost life savings or significant amounts of money and businesses which have collapsed due to their exploitation through this crime type.

It has been approved that the organisations most effective response to tackling the threat and risks posed by fraud will be achieved through the following 'building blocks' approach:

1. Incorporate the UK Fraud Strategy
2. Joining FCCRAS (Fraud and Cyber Crime Reporting and Analysis System)
3. Delivering new Cyber & Fraud Target Operating Model
4. Formalising Multi-Agency Fraud Triage Hub (Reactive)
5. Developing Partnership Cyber Fraud Centre (Proactive)
6. International Law Enforcement Integration

1. UK Fraud Strategy

The UK Fraud Strategy entitled 'stopping scams and protecting the public' was launched by the Home Office on 3 May 2023, and announced the UK Government's ambition to reduce fraud by 10% by 2025. It sets out how this can be achieved under a three pillar approach (Pursue Fraudsters, Block Fraud, Empower People).

National Policing Strategy for Fraud, Economic and CyberCrime

The National Policing Strategy has been released (Nov-2023) to serve as the implementation plan for UK policing to improve the response to fraud, economic and cybercrime through the delivery of key cross cutting strategic objectives.

2. FCCRAS - Fraud and Cyber Crime Reporting and Analysis System

In support of the UK Fraud Strategy, the City of London Police (CoLP) are leading a £30 million Programme of work to replace Action Fraud. The new service, the Fraud and Cyber Crime Reporting and Analysis Service (FCCRAS) will have a public facing brand seeking to deliver a next generation service for fraud and cybercrime reporting and analysis.

It will have enhanced reporting methods with online reporting and call centre support, victim assessment and triage, record management and onward distribution to the appropriate law enforcement agencies.

The service is being designed to improve the flow of intelligence, information and crime reports through the ecosystem. It will improve services to the public, utility by all agencies, and increase the quality of information.

The replacement service will be launched across England and Wales in March 2024. The aspiration is to produce a UK trusted brand for fraud response and take the approach of 'every report matters'.

In terms of the reduction of demand, through benchmarking with the FCCRAS Programme Team it is predicted that by joining the Service, when fully implemented and functioning will reduce Police Scotland fraud call demand by 80% (approx. 17,000 calls based on 2022/23 recorded crime) with the remaining 20% (approx 3,400) that require a police response action and these are calls relating to ongoing crimes, vulnerability and threats to life.

A project will be stood up to consider the introduction of the service into Police Scotland, from Spring 2025.

3. Cyber & Fraud Target Operating Model

PDWP have been are responsible for coordinating the enhancement of Police Scotland's ability to tackle cyber fraud.

In response, PDWP have stood up a group named as the 'Fraud Strategy and Operating Model Coordinating Group' which has brought together key internal stakeholders.

The co-ordination group has the collective vision of bringing about the holistic change necessary to become a centre of excellence in the reporting and triage of fraud related crimes in Scotland. This work is helping to shape the future target operating model (incorporating our membership with FCCRAS).

The baseline target operating model structure consists of a National Co-ordination Unit to provide organisational oversight and consistency in addition to Regional / Divisional Hubs to provide support and robust assessments of recorded crime prior to dissemination to local officers for investigation.

4. Multi-Agency Fraud Triage Hub

Police Scotland fully recognise that there are multiple agencies and organisations who have a footprint in cyber enabled/dependent crime including the response, investigation and intelligence. This includes organisations such as Cyber Scotland, the Scottish Cyber Coordination Centre (SC3) and Cyber and Fraud Centre Scotland.

There is therefore a need for Police Scotland to continue to collaborate across the entire cyber sector in Scotland, to pull together the collective resources, so that we become more than the sum of our parts.

In support of this and to enhance stakeholder engagement, ACC Andy Freeburn as Chair of the Strategic Fraud Governance Group with partners from Scottish Government, the banking and financial sector and the Cyber and Fraud Centre Scotland, have commenced a Multi-agency Fraud Triage Hub pilot, with the objective of ensuring that we work in collaboration to tackle and prevent this escalating threat. The group meet on a weekly basis and report into the Fraud Strategic Governance Group.

Since its inception, this collaborative approach has grown and developed into a highly effective function, which has seen clear tangible successes and outcome as a result. This includes incidents of fraud valuing over £10million having been collectively worked on and £3million of this has been either stopped or recovered.

In addition to the proactive work instigated by the group, a result of the real time sharing of information and intelligence around emerging fraud trends and methods has helped identify innovative and effective disruption, intervention and prevention opportunities whilst safeguarding and identifying appropriate support for victims. This approach ultimately reduces demand on front line policing resources, partner resources and has improved criminal justice outcomes. These activities and outcomes contribute/deliver to objectives under each of the 3 pillars of the UK Fraud Strategy.

Cyber and Fraud Centre Scotland are currently exploring funding opportunities with a view to making the Multi- Agency Financial Crime Triage Hub a permanent and key part of Scotland's response to tackling fraud.

5. Partnership Cyber Fraud Centre

Serious Organised Crime Groups (SOCGs) commonly undertake social engineering to commit fraud, large-scale fraudulent schemes, excise duty evasion and credit card fraud. Cryptocurrency investment fraud is an ongoing concern. Fiscal fraud is prevalent in Scotland, particularly tobacco and alcohol fraud.

The Scottish Crime Campus (SCC), Gartcosh is a critical asset to Police Scotland and is home to many functions of the Specialist Crime Division, Forensic Services and key partner organisations including COPFS, HMRC and the NCA.

With aim of enhancing collaboration in the fight against serious organised crime, each partner brings unique skills and expertise, working together with a common purpose, protecting the people of Scotland and defeating the criminal in an ever more complex world.

Building on the success of the current campus model and close working relationships, consideration is being given to the creation of a proactive cyber and fraud hub where partners will be co-located and tasked with tackling the risk posed by cyber and fraud. This will allow for new standards to be set in intelligence sharing, planning, evidence gathering and enforcement through our combined efforts, expertise and resource.

6. International Law Enforcement Integration

In addition to the foregoing with regards to the overarching objective of keeping Scotland's people, communities, businesses and assets safe in both the physical and digital world Scotland. Numerous cyber threat assessments produced by the National Cyber Security Centre (NCSC), the National Management Centre and other departments across government site significant and escalating risks of cyber-attacks on the police digital estate and policing supply chain whether at a local, regional or national level.

Significant ransomware attacks took place on the UK policing supply chain, where companies in possession of policing data suffered large scale data breaches, resulting in private information pertaining to victims of crime, suspects and other members of the public being published on the dark web. It is clear that such attacks are likely to continue and have the potential to impact right across policing. For this reason, Police Scotland have been working collaboratively with the City of London Police and NPCC to explore how to further forge closer links and collaboration and are now integrated into the UK 24/7 CSI Gold Chief Officer Cadre as part of Operation DA1 (Defend As One).

These close working relationships will continue with the ambition of creating a fully integrated Law Enforcement Model to tackle cybercrime. The benefits of such an approach include efficient working arrangements between law enforcement agencies, early identification and response to emerging threats. In addition, as an organisation it will enable us to be confident, capable and resilient in the fast moving digital world.

To fully maximise the opportunities, we will look to become actively involved in broader initiatives and leverage support and access to funding.

Ethical Approach to the Introduction of New Technology

The principle of policing by consent is fundamental to the Scottish policing model. Providing everyone with a fair, just and effective policing response is our moral responsibility and legal duty. It is an operational imperative to maintain and build the crucial bond of trust with our communities from which we draw our legitimacy.

As previously outlined, the rapid and continuous developments in technology create both challenges and opportunities for policing.

The introduction of technology by the organisation, contributes to ensuring that it is equipped for policing in an ever developing, digitally dependant age while keeping pace with law enforcement agencies across the UK and beyond.

Right Based Pathway

The purpose of the Rights Based Pathway is to meet commitments in the Joint Strategy, Cyber Strategy, the Emerging Technologies Independent Advisory Group (ETIAG) recommendations and the Police Scotland and Scottish Police Authority (SPA) Memorandum of Understanding (MOU), to support decision making and to maintain public trust and confidence in the organisation in respect of it adoption and use of technology.

"The Joint MOU will apply to new and emerging areas of strategy, policy or practice, but the use of the Protocol should lead to the identification of broader, thematic, issues for policing meriting broader strategic discussion. ***For example, Police Scotland may seek to introduce new technologies to protect citizens against the growing range of digital threats and risks. There is, however, the need for a wider, contextual, discussion about the appropriate balance of duties of policing in Scotland, alongside the safety and privacy expectations and rights of the public."***

Police Scotland understands the need to ensure public confidence and appropriate safeguards in utilising such technologies, however the challenge is to balance this against our statutory obligations in keeping the public safe, whilst making best use of available technologies to assist us in this mission.

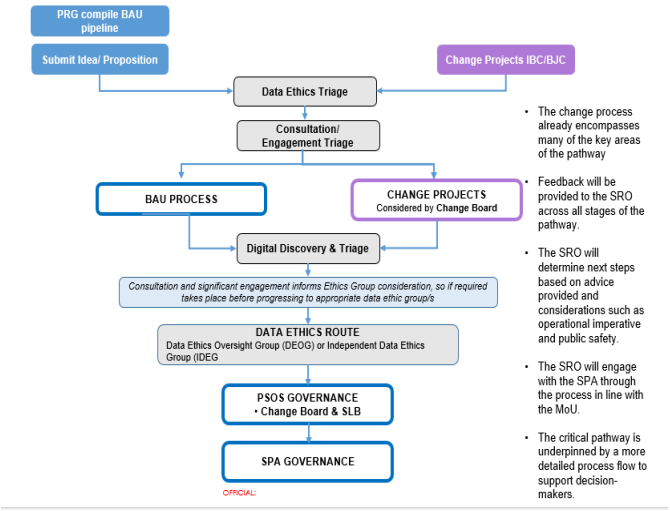
This has been echoed by the SPA who are seeking to ensure that we have a balance of governance to introduce new technology. The Rights Based

Pathway is therefore the mechanism for us to deliver against the terms of the MOU.

A Data Ethics Triage process has been implemented that will assess all data related and data driven technology projects that go through Police Scotland's Change process. The triage process will identify where ethical challenges may lie, provide a pathway to enhanced internal and external scrutiny and provide advice to projects to ensure that data and data driven technology is used legally and ethically.

The Triage process is an integral part of the Rights Based Governance Pathway to ensure that Police Scotland can demonstrate a consistent and proportionate approach to assessing data ethics and public interest considerations.

There has been extensive engagement and support internally and externally throughout the development of this process which can outlined below.



The relevant assurances required from the technologies introduced will be incorporated into the current Digital Forensics Performance framework, with a focus on measuring how effective, efficient they are, in addition to assessing the impact on the wellbeing of our people.

CAID (Child Abuse Image Database) Facial Matching (FM) and the vehicle software BERLA were the first technologies to be introduced to help test, evaluate and evolve the pathway.

CAID FM

CAID as outlined previously is managed by the Home Office and contributes to the fight against Online Child Sexual Abuse and Exploitation (OCSAE). It helps identify and safeguard victims, makes investigating Child Sexual Exploitation and Abuse faster and more effective and supports international effort to remove images from the internet.

As part of the continuous improvement of CAID, a 'Facial Matching' (FM) capability was introduced. In simplistic terms, FM seeks to automatically identify if the image of a person is present within the database, when uploaded by a law enforcement agency.

Assurance - The introduction of this capability has brought about efficiencies in respect of taking less time to review images. A case with 10,000 images would typically take up to 3 days. Now, after matching images against CAID, a case of a similar size can be reviewed in an hour. This has helped shift the balance between reviewing images to identifying victims, with the overarching aim of safeguarding children.

BERLA

Modern cars hold a wide range of information in their computing systems which can be of significant use to an investigation. BERLA will increase our capability to obtain information from motor vehicles as part of serious crime investigations. This software allows for the access and assessment of data from vehicles.

Assurance - Access to this capability is governed as part of our Digital Device Examination and Triage process through the Cybercrime Gateway whereby all requests are scrutinised and considered for approval in line with Police Scotland's Digital Forensic Examination Principles.

Since it went live in late 2023 there have been 16 approved requests for use of the software in relation to 20 vehicles. This includes a high profile murder and a multimillion pound fraud linked to international serious and organised crime.

On 9 February 2024 and following approval at the Policing in a Digital World Programme Board, the following technologies, which have been subject to the robust Rights Based Pathway process, were approved for use.

CAID Image Classifier

CAID Image Classifier is an assisted decision making tool for analysts grading images on CAID and is an add-on solution within the existing platform which is used to detect and classify IIOC from suspect devices.

It does not make decisions, the classification and assessment remains the sole responsibility of the analyst and it is their role to confirm the grade they determine best fits the image regardless of the suggested grade provided by the classifier. The analyst will then confirm the grade of every image before uploading to CAID.

Police Scotland Digital Forensics have been afforded the opportunity to test the technology and using 18 million images found it to be about 90% accurate. This was completed in 1 day and which currently would take an analyst several months to achieve.

Between September 2022 and September 2023 Police Scotland seized and examined 1478 digital devices within the Digital Forensics Laboratories in relation to OCASE investigations.

Given the metrics quoted and tested, the introduction of this technology will make us more efficient and effective with our processes and improve the wellbeing of our staff employed in this area.

A survey carried out by the Home Office in 2022 provided the following anecdotal support:

"It helps pull important content out - we would of found these images but it would of taken us weeks."

"Before it was a case of going through hundreds or thousands of images manually; now the classifier helps us get to the images we need to prioritise which is really valuable. It allows officers to make those sort of fast time decisions about safeguarding rather than a couple of days later or weeks later when they have had time to sort through large numbers of images"

"Average time saved by using the tool is between 60-80%"

Cyacomb Examiner Tool

Cyacomb Examiner is a fast forensic triage (FFT) tool, designed for the on scene triage of computers and computer peripheral devices including laptops, hard drives and external storage devices

It has been procured by the Home Office for use by law enforcement agencies across the UK and seen as a "tool in the box" for digital forensic investigators.

The product/software when inserted into the relevant device, searches across live and deleted files to find and highlight any images relating to Indecent Images of Children (IIOC). In terms of Police Scotland's use this will be specific to the Child Abuse Image Database (CAID).

Through their evaluation of the product and in assisting Police Scotland with its introduction, the Home Office provided the following feedback from a law enforcement agency:

""We had a great Cyacomb Examiner hit this morning with the three filters finding 32 video files. The tool worked flawlessly within 57 seconds on a 250gb SSD drive."

All technologies introduced through the pathway to date, have been procured by the Home Office and at no cost to Police Scotland.

The benefits and assurances of all technologies introduced will be incorporated into the current Digital Forensic Performance framework in terms of their effectiveness, efficiency and impact on the wellbeing of our people.

Artificial Intelligence (AI) in Policing

The rapid growth of Artificial Intelligence (AI) within policing is unsurprising. The speed and accuracy that AI could bring to police processes make it an attractive way to deliver an effective and efficient service. However its application of AI can be contentious if not properly explored and consulted on.

Police Scotland are currently engaging both internally and externally with a number of partners including the NPCC, SPA and Scottish Biometrics

Commissioners with regards to the use of AI and the following aspects:

- Strategy & Policy
- Practical use of AI
- Assurance & Scrutiny

These have also formed the basis of previous Research and Evidence Forums facilitated by the SPA.

On 19 June 2024, The Scottish Biometrics Commissioner, the Scottish Police Authority and Police Scotland will be hosting a symposium entitled **"**Biometrics in Criminal Justice: Exploring and Understanding the use of biometrics in Scotland*".*

The event will consider the use and benefits of biometric technology by law enforcement while promoting a lawful and ethical approach to the use of these technologies.

GLOSSARY

A
ACC – Assistant Chief Constable
AI – Artificial Intelligence

C
CAID – Child Abuse Image Database
CHP – Cyber Harm Prevention
CCS – Cyber Choices Scotland
CMA – Computer Misuse Act
CoLP – City of London Police
COPFS - Crown Office and Procurator Fiscal Office
CS – Chief Superintendent
CTSA – Counter Terrorism Security Advisor

D
DCC – Deputy Chief Constable
DDD – Data Drives Digital
DEDD – Digital Evidence Detection Dog
DF Digital Forensics
DICE - Darkweb Intelligence Collection and Exploitation Unit

E
ETIAG - Emerging Technologies Independent Advisory Group

F
FCCRAS - Fraud and Cyber Crime Reporting and Analysis System)
FM – Facial Matching
FFT - Fast forensic triage

H
HMRC – Her Majesty's Revenue and Customs

I
IIOC – Indecent Images of Children
IIU – Internet Investigations Unit

M
MOU – Memorandum of Understanding

N
NCA – National Crime Agency
NCRAB – National Cyber Resilience Advisory Board
NCSC – National Cyber Security Centre
NPCC – National Police Chiefs Council

O
OCSAE- Online Child Sexual Abuse and Exploitation
OSINT – Open Source Intelligence

P
PCA – Police Cyber Alarm
PDWP – Policing in a Digital World Programme
PPCW – Partnerships, Prevention and Community Wellbeing
PRG – Professional Reference Group

R
RBP – Rights based Pathway
RDOT - Regional Darkweb Operations Teams
ROCU – Regional Organised Crime Unit

S
SCC – Scottish Crime Campus
SC3 - Scottish Cyber Coordination Centre
SME - Small & Medium Enterprises
SOBC –Strategic Outline Business Case
SOCG - Serious Organised Crime Groups
STEM Science Technology Engineering and Maths
SSD – Solid State Drive
SPA- Scottish Police Authority
STRA – Strategic Threat and Risk Assessment

T
TOR – The Onion Router

U
UKAS - United Kingdom Accreditation Service

V
VAWG – Violence Against Women and Girls