

Cyber-Scotland Conference

23rd February 2021

All the recordings can be viewed at <https://www.eicc.co.uk/pscr21/event-main-page/>. Session 1 will be of most interest to community safety practitioners.

Some highlights from the morning's presentations:




- Launches:
 - o Police Scotland cyber strategy
 - o Launch of new Digital strategy for Scotland will be happening soon (consultation closed on 23rd December 2020). Colin Cook, Scottish Government input.
 - o New cyber partnership: <https://digit.fyi/cyberscotland-partnership-to-support-cyber-resilience/>

Input on the categories of harms caused by cyber attacks

Ciaran Martin, SBRC Board member

- Cyber is a domain but also an environment
- Cyber-infrastructure is as important as electricity cables, water supply and other utilities.
- Should not sit within IT alone in an organisation

Cyber Attacks: Categories of Harms Caused

 Getting Robbed	 Getting Weakened	 Getting Hurt
Cash Theft IP Theft Data Theft	Espionage Political Interference Prepositioning	Destructive Ransomware Catastrophic *

September 2020 © Ciaran Martin 2020

- 'Getting robbed' can be anything from little amounts of money to state-sponsored bank robberies with vast amounts of money causing systemic issues.
- What damage does data theft do? What harm does it cause? E.g. selling data to perpetuate ID theft.
- Defences are too weak, incentives to pay, other countries let criminals like this operate.
- And don't forget about the aggregation of these small harms.

Suggestion of a discussion that Boards should be having re cyber-security:

5 QUESTIONS FOR AN INFORMED BOARD DISCUSSION

- How do we defend our organisation against phishing attacks?
- How does our organisation control the use of privileged IT accounts?
- How do we ensure that our software and devices are up to date?
- How do we make sure our partners and suppliers protect the information we share with them?
- What authentication methods are used to control access to systems and data?

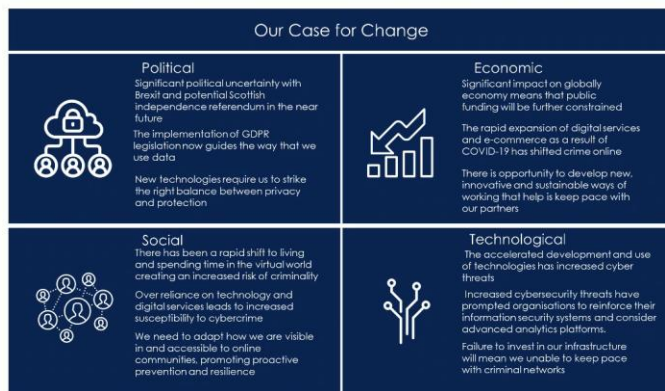
<https://www.ncsc.gov.uk/guidance/board-toolkit-five-questions-your-boards-agenda>

Key recommendation from the speaker: Have a strategy that assumes some of these phishing attacks work, not just educating staff not to click on suspect emails.

Scotland's investment in cyber is actually very small – there is a lot of work to shine a light and attract more investment and attention to this area.

Malcolm Graham, Police Scotland – new cyber strategy

Cyber Strategy – Case for Change



- The need for a new approach to cyber is driven both internally and externally:
 - Demands faced in policing are becoming increasingly complex and the resources available to meet these demands continue to be stretched
 - We need to adapt and change to provide a relevant effective modern policing service, fit for the digital age, which builds and maintains public confidence
 - The rapid pace of political, economic, societal and technological change means that we must continually adapt to meet the needs of the communities we serve
 - It is imperative that Police Scotland transitions to be able to embrace current and future challenges that the digital age presents

Cyber Strategy – Threat & Risk

Very High Operational Priorities	Drugs Supply/Drugs Harm
	Child Sexual Abuse
	Serious Violence/Homicide
	Human Trafficking
	Rape
	Counter Terrorism
High Operational Priorities	Adult Protection
	Serious Organised Crime
	Domestic Abuse
	Missing Persons
	Management of Registered Sex Offenders
	Public Order/Safety
	Road Casualties
	Fraud

- Our Strategic Threat Assessment (2020-2023) is a risk based assessment of operational policing issues combined with an organisational assessment of our approach, capability and capacity to support the delivery of policing services
- Technology presents significant threat AND opportunity - Police Scotland recognise the threats posed by criminality that takes place online and the organisational need to prioritise investment in our capability and capacity to tackle the broad range of criminality presenting in the digital age.
- Connected to this is the requirement to ensure Police Scotland and its ICT and data assets are fully protected from all cyber security threats
- Current Very High/High Operational Priorities are shown in the table, 'Cyber' cuts across majority of these priorities, whether it be Cyber Dependent or Cyber Enabled, the key online threats are:
 - Sexual Offences/CSA
 - Financial & Economic Crime
 - Threatening Behaviour & Communication Offences
 - Offences under Computer Misuse Act 1990 (including data breaches, hacking or denial of service)

Cyber Strategy – Key Activity to Date

Cyber Capabilities Programme	<ul style="list-style-type: none"> • Introduction of Cyber Champions, identifying staff internally that possess 'cyber' skills and knowledge and utilising that knowledge and experience to increase capabilities • Delivery of Cyber Kiosks (Phase 1) • Delivery of an enhanced, informed Consent process across the Force • Introduction of Cyber Markers - System enhancements and raising awareness around the importance of accurately recording cyber crime to help identify trends and improve our response • Delivery of a modern, replacement Case Management System for Digital Forensics and Cyber Investigations is in progress • Planning and scoping for our ISO 17025 accreditation journey for Digital Forensics has recently commenced
Partnership Prevention & Innovation	<ul style="list-style-type: none"> • Annual and monthly Cyber Threat Assessments published taking into consideration Police Scotland and national law enforcement perspectives • Introduction of a Digital Skills Academy (DSA) formed in conjunction with National Crime Agency and Cisco, DSA is a collaboration between industry and law enforcement to deliver a wide range of digital training to upskill our people • A refresh of the Probationer training programme is underway with a focus on policing in a digitally enabled age • Scottish Business Resilience Centre Cyber Incident Response – Mapping of key milestones of any cyber incident, who the primary parties involved are, and a description of the work carried out in each section. Assessment of the areas of weakness in the milestone map

OFFICIAL



A sense from a number of speakers that they were speaking to the converted at this conference – not sure the cyber strategy (or digital issues more broadly) has actually landed where it needs to yet in other places like government, public sector etc.

As part of cyber-Scotland week the SCCJR published a paper on the reality of Cyber-awareness:

This briefing paper represents a summary of doctoral research that explores how different groups make sense of and respond to cybercrime in their everyday lives.

The research found that people from different groups, places, and times think about cybercrime and cybersecurity in different ways.

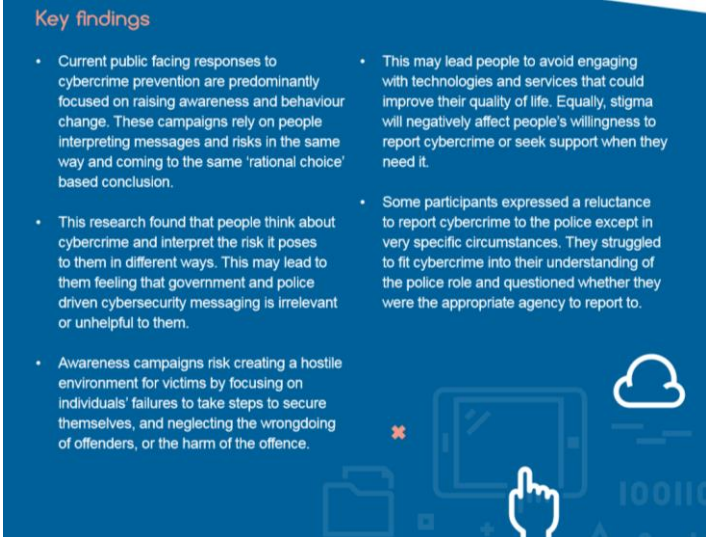
This has implications for government and police awareness raising campaigns.

Population-level awareness

campaigns designed to communicate 'simple' messages may get lost in translation or disregarded because they do not resonate with the social and cultural contexts of their target audiences.

After considering the challenges government and police face, the report imagines possible future directions for cybersecurity awareness raising that may enable them to be more sensitive to local social cultural contexts and foster the creation of communities of supportive cybersecurity.

Read the full paper at <https://www.sccjr.ac.uk/wp-content/uploads/2021/02/Dr-Shane-Horgan.pdf>

A blue graphic titled "Key findings" containing a bulleted list of research results. The text is white on a blue background. The list includes points about public responses to cybercrime prevention, the impact of awareness campaigns, and the reluctance to report cybercrime to the police. The graphic also features faint icons of a hand pointing at a screen, a cloud, and binary code.

Key findings

- Current public facing responses to cybercrime prevention are predominantly focused on raising awareness and behaviour change. These campaigns rely on people interpreting messages and risks in the same way and coming to the same 'rational choice' based conclusion.
- This research found that people think about cybercrime and interpret the risk it poses to them in different ways. This may lead to them feeling that government and police driven cybersecurity messaging is irrelevant or unhelpful to them.
- Awareness campaigns risk creating a hostile environment for victims by focusing on individuals' failures to take steps to secure themselves, and neglecting the wrongdoing of offenders, or the harm of the offence.
- This may lead people to avoid engaging with technologies and services that could improve their quality of life. Equally, stigma will negatively affect people's willingness to report cybercrime or seek support when they need it.
- Some participants expressed a reluctance to report cybercrime to the police except in very specific circumstances. They struggled to fit cybercrime into their understanding of the police role and questioned whether they were the appropriate agency to report to.