THE CHALLENGE TO POLICING IN INVESTIGATING CYBERCRIME

DI Eamonn Keane
Head of Cyber Security & Innovation
Scottish Business Resilience Centre
Police Scotland

Cyber Science 2018
IEEE
Glasgow
Agenda

Strategy - A more resilient world!
The growing threat landscape!
Law Enforcement challenges.
Investment in Education! Education!
Prevention V Detection!
Practical Advice!!
Q & A.

POLICE SCOTLAND
SAFE, SECURE AND PROSPEROUS: A CYBER RESILIENCE STRATEGY FOR SCOTLAND

Public Sector

Action Plan 2017-18

Implementation

This toolkit has been produced to accompany
It is intended to be a live document

Please send all comments to:

www.gov.scot/cyberresilience

Learning & Skills Action Plan for Cyber Resilience 2018-20

Produced by the National Cyber Resilience Leaders’ Board
In partnership with the Scottish Government
Why we do what we do?

The Scottish & UK government is committed to making the UK a secure and resilient digital nation.

A key aspect of this strategy is through robust engagement and an active partnership between government, industry and law enforcement to significantly enhance the levels of cyber security across UK networks.
The Ambition
Safe, secure and prosperous: Scotland’s cyber resilience strategy

4 Overarching Principles

A. Increase people’s cyber resilience through awareness raising and engagement.

B. Explicitly embed cyber resilience throughout our education and lifelong learning system.

C. Increase people’s cyber resilience at work.

D. Develop the cyber security workforce and profession to ensure that skills supply meets demand and that skilled individuals can find rewarding employment in Scotland.

Critically Important
Addressing The Skills Shortage

Skills shortage threatening UK cybersecurity 'could last for 20 years'

Summary: A report into the UK's Cyber Security Strategy has found that a lack of workers with the right security skills is making it difficult for the country to defend itself online.
National Audit Office warns UK needs more skilled cyber-crime fighters

A lack of skilled workers is hampering the UK's fight against cyber crime, the National Audit Office (NAO) has warned.

The spending watchdog had heard from experts who believe it could take "up to 20 years to address the skills gap", it said in a report.

"Progress has been made in tackling cyber fraud, with more police resources and prosecutions aimed at catching cyber criminals", the NAO added.

But the government said it was "investing heavily" in research and education.

"The number of IT and cyber security professionals in the UK has not increased in line with the growth of the internet, the watchdog said.

Labour said the report highlighted the lack of support for "the next generation of British cyber security experts".

In 2011, ministers announced funding of £650m to implement the UK's Cyber Security Strategy, which set out the risks of the UK's growing reliance on cyber space.
Cyber Apprenticeships!

QA Apprenticeships launches Cyber Security programme in Scotland

Rarely a week goes by without another hack reaching the headlines. News of corporations being digitally infiltrated and customer data being stolen has, unfortunately, become too commonplace. It seems that as our reliance on technology to give us a ‘connected society’ has increased, ironically though understandably, we have become more vulnerable to cyber attacks.

It’s no surprise then that Scotland’s cyber security sector is rapidly growing and has become an increasingly high profile area of the IT industry. Last year a shocking 81% of large corporations and 60% of small businesses in the UK reported a cyber-breach, with the cost for the worst breach estimated between £600,000 to £1.15 million for large businesses, and £65,000 to £115,000 for smaller ones.

Can ‘Digital Nation’ protect the future of the Scottish economy?
Scottish skills programme looks for a new generation of cyber crime fighters

by Will Peakin / November 9, 2017 / Education, News, People, Society

Skills Development Scotland (SDS) is launching an initiative to encourage school pupils to choose fighting cyber crime as their ideal career choice. Aimed at young people from S1 to S3, the Cyber Skills Programme aims to create a new generation of “white hat” hackers by raising skill levels and awareness of the growing number of jobs in this fast paced, super secret industry.

Kicking off at today’s STEM Festival at Glasgow Science Centre, the programme will see a series of fun and engaging events
SICSA Launches the Cyber Nexus Virtual Innovation Hub

As part of the recent Scottish Government funding for the SICSA Cyber Nexus, we have recently launched the Cyber Nexus Virtual Innovation Hub. This funding programme will support innovative research in Cyber Security that has commercial potential.

The main aim of this initiative is to help researchers to develop their technologies into a proposition that can either be licensed to existing companies or spun-out into a new start-up venture. Up to £3K is available for each successful applicant.

We are now accepting applications from researchers at SICSA member institutions. For more details and to apply, please visit our Cyber Nexus Virtual Innovation Hub page.

If you have any questions about this funding, please contact admin@sicsa.ac.uk.
Scotland's Future & Everyone's Future

• International Collaboration
• Government – Industry – Academia Collaboration
• Joint Working – Intelligence, Technical, Disruption
• Prevention/ Education
• Curriculum for 21st Century
• Upskill Children & Wider Population
• Target Harden Existing Business
• SBRC Role
• Cyber Security Grow as Industry Sector

Cyber Services:

**Individual Footprint**
Find out what exists about you online and how this could be used against you.

**Corporate Footprint**
Find out what information an attacker can gather about your business.

**Remote Testing**
Can an attacker breach your system remotely?

**Internal Testing**
Find out how secure your network is once an attacker has managed to make a connection.

**Web Application Testing**
How secure is your website? Find out what vulnerabilities exist and how to close them.

**Table Top Exercise**
Scenario based exercises designed to test how well you would cope with a Cyber attack.

**Awareness Training**
Ensure your staff are aware of risks faced from Cyber and how to protect themselves and your business.

**Security Policy Review**
Find out how robust your current Cyber Security policies are.

**SwiftPass**
Monitor email addresses and get a rapid notification if it is found in a data breach.
Scotland as a cyber world leader!

Really?
SCOTLAND’S CYBER DEPOT

1. TIER 1 – TRIAGE APPRENTICES / GRADUATES
2. TIER 2 – SOC / TRUSTED PARTNERS
3. TIER 3 – ACADEMIA / R & D
4. TIER 4 – SCOTLAND’S TECH COMMUNITY DEVELOPMENT
5. TIER 5 – POLICE / SENIOR TECH COMMUNITY / INVESTIGATIONS
6. TIER 6 – SG/NCSC EUROPOL
Cyber Regional Organised Crime Units

NCCU

MPS Operation Falcon

EUROPOL

EC3 | European Centre

FBI

POLICE SCOTLAND
“I can do more damage on my laptop in my pyjamas, before my first cup of Earl Grey, than you can do in a year in the field.”

Q - Skyfall
Criminal Investigators - Detectives

JUST ONE MORE THING.........

POLICE SCOTLAND
So how has the threat changed in the last 5 years?
Criminal & malicious activity
The Usual Suspects!

- Malware
- Phishing
- Ransomware
- Hacker
- Social Engineering
More than £2m lost to vishing fraud

Almost £2.5m has been lost to fraudsters in vishing and spoofing scams targeted at Highlands businesses, police have said.

The firms received calls from people claiming to work for their banks and telling them their account had been compromised.

Police Scotland said the incidents, which saw a number of firms targeted, happened between 19 and 30 July.

The force said the fraudsters used "genuine-looking communications".

Businesses have been urged not to make any transactions if they receive such calls and to instead call their bank using a different phone to the one the initial call was received on.

Det Insp Iain McPhail, of Police Scotland’s Economic Crime and Financial Investigation Unit, said: "These fraudsters are very convincing and have managed to obtain a significant amount of money from local businesses.

"We have launched a thorough investigation into these incidents and are working with the companies’ relevant banks.

"Some of the money that companies have lost has been recovered and work is ongoing to try and recover as much money as possible."
NEED HELP unlocking your digital life without paying your attackers*

YES  NO

Ransomware is malware that locks your computer and mobile devices or encrypts your electronic files. When this happens, you can’t get to the data unless you pay a ransom. However, this is not guaranteed and you should never pay!
Saudi Aramco’s Khurais plant. A cyber attack wiped out data on three-quarters of Aramco’s PCs.
In August 2017, a petrochemical company with a plant in Saudi Arabia was hit by a new kind of cyber attack. The attack was not designed to simply destroy data or shut down the plant, investigators believe. It was meant to sabotage the firm’s operations and trigger an explosion.
Timeline: How Stuxnet attacked a nuclear plant

Invisible weapon

Iranian President Mahmoud Ahmadinejad during a tour of centrifuges at Natanz in 2008.

In four steps, Stuxnet infiltrated a nuclear factory, went undetected, then mounted the worm and destroyed its target.
WikiLeaks implied the hack was by its supporters.

Was Russia Behind the Massive Dyn DDoS Cyber Attack?
Is this cybercrime?

Britain Sees First Bitcoin Armed Robbery: Reports

The robbery happened on January 22 at the couple's home in the village of Moulsford in southeast England, according to the Daily Mail, which said the cryptocurrency crime was the first of its kind.

World | Agence France-Presse | Updated: January 29, 2018 19:53 IST

· Nosey Grandson Stumbles Upon His Grandmothers Hidden Safe, Then He Broke it Open (LifeDaily.com)

· Play this Game for 1 Minute and see why everyone is addicted (River Combat)

TRENDING

Xiaomi Redmi 5 Gets a New Variant, Features 4GB of RAM
Here's How Hackers Stole $80 Million from Bangladesh Bank

Monday, March 14, 2016 | Swati Khandelwal
Crimes in the Darknet

- Human Trafficking
- Drug Dealing
- Hacking
- Access to Government Sites
- Information Theft
- Illegal Transactions

- Selling Guns
- Assassination
- Child Pornography
Dear Customer,

Your Shipment arrived at the post office today. Our courier was unable to deliver the Shipment to your address. To receive your Shipment, Please Visit the nearest DHL office and take your Shipment label attached in this email.

Attached is the Electronic Proof (s) of your Shipment and document. Check attachment for Shipping Label. Please print and show at the nearest DHL office to receive your Shipment.

With kind regards,

DHL Express Team
ORGANISED CRIME

The New Face of Organized Crime

Hackers are no longer lone wolves. They're now banding together to run fewer—yet much larger—attacks, similar to the traditional crime rings of the 20th century.

80% of cyber-attacks are driven by organized crime rings, in which data, tools, and expertise are widely shared.¹

POLICE SCOTLAND
Feezan Hameed

£113 million Frauds

Vishing / Social engineering of banking customers.

Data acquired including account details/passwords.

Money transferred online – mule account networks.

UK wide investigation.

Numerous UK Law Enforcement agencies.

Arrested in Paris on false passport

Convicted and sentenced to 11 years imprisonment
Serious Organised Crime Gangs

OFFICIAL: NONE

Serious Organised Crime Gangs

OFFICIAL: NONE

Serious Organised Crime Gangs

OFFICIAL: NONE

Serious Organised Crime Gangs

OFFICIAL: NONE

Serious Organised Crime Gangs

OFFICIAL: NONE

Serious Organised Crime Gangs

OFFICIAL: NONE

Serious Organised Crime Gangs

OFFICIAL: NONE

Serious Organised Crime Gangs

OFFICIAL: NONE

Serious Organised Crime Gangs

OFFICIAL: NONE

Serious Organised Crime Gangs

OFFICIAL: NONE

Serious Organised Crime Gangs

OFFICIAL: NONE

Serious Organised Crime Gangs

OFFICIAL: NONE

Serious Organised Crime Gangs

OFFICIAL: NONE

Serious Organised Crime Gangs

OFFICIAL: NONE

Serious Organised Crime Gangs

OFFICIAL: NONE

Serious Organised Crime Gangs

OFFICIAL: NONE

Serious Organised Crime Gangs

OFFICIAL: NONE

Serious Organised Crime Gangs

OFFICIAL: NONE

Serious Organised Crime Gangs

OFFICIAL: NONE

Serious Organised Crime Gangs

OFFICIAL: NONE

Serious Organised Crime Gangs

OFFICIAL: NONE

Serious Organised Crime Gangs

OFFICIAL: NONE

Serious Organised Crime Gangs

OFFICIAL: NONE

Serious Organised Crime Gangs

OFFICIAL: NONE

Serious Organised Crime Gangs

OFFICIAL: NONE

Serious Organised Crime Gangs

OFFICIAL: NONE

Serious Organised Crime Gangs

OFFICIAL: NONE

Serious Organised Crime Gangs

OFFICIAL: NONE

Serious Organised Crime Gangs

OFFICIAL: NONE

Serious Organised Crime Gangs

OFFICIAL: NONE

Serious Organised Crime Gangs

OFFICIAL: NONE

Serious Organised Crime Gangs

OFFICIAL: NONE

Serious Organised Crime Gangs

OFFICIAL: NONE

Serious Organised Crime Gangs

OFFICIAL: NONE

Serious Organised Crime Gangs

OFFICIAL: NONE

Serious Organised Crime Gangs

OFFICIAL: NONE

Serious Organised Crime Gangs

OFFICIAL: NONE

Serious Organised Crime Gangs

OFFICIAL: NONE

Serious Organised Crime Gangs

OFFICIAL: NONE

Serious Organised Crime Gangs

OFFICIAL: NONE

Serious Organised Crime Gangs

OFFICIAL: NONE

Serious Organised Crime Gangs

OFFICIAL: NONE

Serious Organised Crime Gangs

OFFICIAL: NONE

Serious Organised Crime Gangs

OFFICIAL: NONE

Serious Organised Crime Gangs

OFFICIAL: NONE

Serious Organised Crime Gangs

OFFICIAL: NONE

Serious Organised Crime Gangs

OFFICIAL: NONE

Serious Organised Crime Gangs

OFFICIAL: NONE

Serious Organised Crime Gangs

OFFICIAL: NONE

Serious Organised Crime Gangs

OFFICIAL: NONE

Serious Organised Crime Gangs

OFFICIAL: NONE

Serious Organised Crime Gangs

OFFICIAL: NONE

Serious Organised Crime Gangs

OFFICIAL: NONE

Serious Organised Crime Gangs

OFFICIAL: NONE

Serious Organised Crime Gangs

OFFICIAL: NONE

Serious Organised Crime Gangs

OFFICIAL: NONE

Serious Organised Crime Gangs

OFFICIAL: NONE

Serious Organised Crime Gangs

OFFICIAL: NONE

Serious Organised Crime Gangs

OFFICIAL: NONE

Serious Organised Crime Gangs

OFFICIAL: NONE

Serious Organised Crime Gangs

OFFICIAL: NONE

Serious Organised Crime Gangs

OFFICIAL: NONE

Serious Organised Crime Gangs

OFFICIAL: NONE

Serious Organised Crime Gangs

OFFICIAL: NONE

Serious Organised Crime Gangs

OFFICIAL: NONE

Serious Organised Crime Gangs

OFFICIAL: NONE

Serious Organised Crime Gangs

OFFICIAL: NONE

Serious Organised Crime Gangs

OFFICIAL: NONE

Serious Organised Crime Gangs

OFFICIAL: NONE

Serious Organised Crime Gangs

OFFICIAL: NONE

Serious Organised Crime Gangs

OFFICIAL: NONE

Serious Organised Crime Gangs

OFFICIAL: NONE

Serious Organised Crime Gangs

OFFICIAL: NONE

Serious Organised Crime Gangs

OFFICIAL: NONE

Serious Organised Crime Gangs

OFFICIAL: NONE

Serious Organised Crime Gangs

OFFICIAL: NONE

Serious Organised Crime Gangs

OFFICIAL: NONE

Serious Organised Crime Gangs

OFFICIAL: NONE

Serious Organised Crime Gangs

OFFICIAL: NONE

Serious Organised Crime Gangs

OFFICIAL: NONE

Serious Organised Crime Gangs

OFFICIAL: NONE

Serious Organised Crime Gangs

OFFICIAL: NONE

Serious Organised Crime Gangs

OFFICIAL: NONE

Serious Organised Crime Gangs

OFFICIAL: NONE

Serious Organised Crime Gangs

OFFICIAL: NONE

Serious Organised Crime Gangs

OFFICIAL: NONE

Serious Organised Crime Gangs

OFFICIAL: NONE

Serious Organised Crime Gangs

OFFICIAL: NONE

Serious Organised Crime Gangs

OFFICIAL: NONE

Serious Organised Crime Gangs

OFFICIAL: NONE

Serious Organised Crime Gangs

OFFICIAL: NONE

Serious Organised Crime Gangs

OFFICIAL: NONE

Serious Organised Crime Gangs

OFFICIAL: NONE

Serious Organised Crime Gangs

OFFICIAL: NONE

Serious Organised Crime Gangs

OFFICIAL: NONE

Serious Organised Crime Gangs

OFFICIAL: NONE

Serious Organised Crime Gangs

OFFICIAL: NONE

Serious Organised Crime Gangs

OFFICIAL: NONE

Serious Organised Crime Gangs

OFFICIAL: NONE

Serious Organised Crime Gangs

OFFICIAL: NONE

Serious Organised Crime Gangs

OFFICIAL: NONE

Serious Organised Crime Gangs

OFFICIAL: NONE

Serious Organised Crime Gangs

OFFICIAL: NONE

Serious Organised Crime Gangs

OFFICIAL: NONE

Serious Organised Crime Gangs

OFFICIAL: NONE

Serious Organised Crime Gangs

OFFICIAL: NONE

Serious Organised Crime Gangs

OFFICIAL: NONE

Serious Organised Crime Gangs

OFFICIAL: NONE

Serious Organised Crime Gangs

OFFICIAL: NONE

Serious Organised Crime Gangs

OFFICIAL: NONE

Serious Organised Crime Gangs

OFFICIAL: NONE

Serious Organised Crime Gangs

OFFICIAL: NONE

Serious Organised Crime Gangs

OFFICIAL: NONE

Serious Organised Crime Gangs

OFFICIAL: NONE

Serious Organised Crime Gangs

OFFICIAL: NONE

Serious Organised Crime Gangs

OFFICIAL: NONE

Serious Organised Crime Gangs

OFFICIAL: NONE

Serious Organised Crime Gangs

OFFICIAL: NONE

Serious Organised Crime Gangs

OFFICIAL: NONE

Serious Organised Crime Gangs

OFFICIAL: NONE

Serious Organised Crime Gangs

OFFICIAL: NONE

Serious Organised Crime Gangs

OFFICIAL: NONE

Serious Organised Crime Gangs

OFFICIAL: NONE

Serious Organised Crime Gangs

OFFICIAL: NONE

Serious Organised Crime Gangs

OFFICIAL: NONE

Serious Organised Crime Gangs

OFFICIAL: NONE

Serious Organised Crime Gangs

OFFICIAL: NONE

Serious Organised Crime Gangs

OFFICIAL: NONE

Serious Organised Crime Gangs

OFFICIAL: NONE

Serious Organised Crime Gangs

OFFICIAL: NONE

Serious Organised Crime Gangs

OFFICIAL: NONE

Serious Organised Crime Gangs

OFFICIAL: NONE

Serious Organised Crime Gangs

OFFICIAL: NONE

Serious Organised Crime Gangs

OFFICIAL: NONE

Serious Organised Crime Gangs

OFFICIAL: NONE

Serious Organised Crime Gangs

OFFICIAL: NONE

Serious Organised Crime Gangs

OFFICIAL: NONE

Serious Organised Crime Gangs

OFFICIAL: NONE

Serious Organised Crime Gangs

OFFICIAL: NONE

Serious Organised Crime Gangs

OFFICIAL: NONE

Serious Organised Crime Gangs

OFFICIAL: NONE

Serious Organised Crime Gangs

OFFICIAL: NONE

Serious Organised Crime Gangs

OFFICIAL: NONE

Serious Organised Crime Gangs

OFFICIAL: NONE

Serious Organised Crime Gangs

OFFICIAL: NONE

Serious Organised Crime Gangs

OFFICIAL: NONE

Serious Organised Crime Gangs

OFFICIAL: NONE

Serious Organised Crime Gangs

OFFICIAL: NONE

Serious Organised Crime Gangs

OFFICIAL: NONE

Serious Organised Crime Gangs

OFFICIAL: NONE

Serious Organised Crime Gangs

OFFICIAL: NONE

Serious Organised Crime Gangs

OFFICIAL: NONE

Serious Organised Crime Gangs

OFFICIAL: NONE

Serious Organised Crime Gangs

OFFICIAL: NONE

Serious Organised Crime Gangs

OFFICIAL: NONE

Serious Organised Crime Gangs

OFFICIAL: NONE

Serious Organised Crime Gangs

OFFICIAL: NONE

Serious Organised Crime Gangs

OFFICIAL: NONE

Serious Organised Crime Gangs

OFFICIAL: NONE

Serious Organised Crime Gangs

OFFICIAL: NONE

Serious Organised Crime Gangs

OFFICIAL: NONE
Spread the social word but maybe not the image!! - Sexting

DEFINITION...

SEXTING

Sending of sexually explicit photos or text through one's mobile phone to friends or potential suitors.

POLICE SCOTLAND
Teenager's death sparks cyber-blackmailing probe

The teenager had been told to pay money into an account or a video or images of him would be made public.

Police in Fife are investigating claims that a 17-year-old boy killed himself because he was being blackmailed on the internet.
Never in Scotland!

Croatian police arrest suspect behind global cyber attack platform

Two Scots arrested after website linked to millions of cyber attacks including against UK banks is shut down
So what are the challenges/threats?

- Global, international, industrial & automated
- Jurisdictional reach & anonymous.
- Increased criminal opportunities.
- Anyone can be (or hire) a cyber criminal!
- Lack of clear & concise statistical data.
- Under reporting
- Technological advances provide opportunities but equally increases the threat of cybercrime - The ‘Internet of Things’
- Social media as an attack vector
- Data Analytics
- Disaster Recovery & Business Continuity
WHO YOU GONNA CALL?

POLICE SCOTLAND
Cyber Resilience is thorough Preparation

Overarching Cyber Security Strategy!
Pre-planned Exercise.
Incident Management & Response Plan.
Communications Strategy.
Investigative Strategy.
Incident Manager & Team
Gold, Silver, Bronze.
Mitigation & Recovery Strategy.
Logistics - Contingency

POLICE SCOTLAND
Key questions that all CEOs & CISO’s should be asking this week?

• "Are we vulnerable to a cyber intrusion, SQL injection, ransomware or DDoS based attacks?“
• "What assurance activity have we done to confirm that we are not vulnerable?“
• "If we were compromised, would an attacker be able to gain access to unencrypted sensitive data?“
• “Are we satisfied have we engaged sufficient 3rd party security provider?"
• “What is our company posture on security?”
• “What and how vibrant is your overarching cyber security policy?“

POLICE SCOTLAND
Incident Management Planning Steps

**Policy**

- Security Incident Management Policy

**Plan**

- Security Incident Response Plan

**Runbooks**

- CAT 1 - Unauthorised Access
- CAT 3 - Malware
- CAT 5 - Ransomware
- CAT 2 - Denial of Service
- CAT 4 - Insider Misuse
- CAT 6 - PCI-DSS
It’s easy to be safe
The Cyber-security Information Sharing Partnership (CiSP), part of CERT-UK, is a joint industry government initiative to share cyber threat and vulnerability information in order to increase overall situational awareness of the cyber threat and therefore reduce the impact on UK business.

CiSP allows members from across sectors and organisations to exchange cyber threat information in real time, on a secure and dynamic environment, whilst operating within a framework that protects the confidentiality of shared information.

CiSP members are also able to receive network monitoring reports. This free service allows users to receive tailored feeds of information from CERT-UK covering any malicious activity that we see on your network.

Users can sign up for this service when they join CiSP or register your interest and a member of the team will get back to you when you have the necessary information.

Fusion Cell
90 Days to DMARC:
The Global Cyber Alliance Challenge

- Month One: November 2017
  - Awareness and Coalition Building

- Month Two: December 2017

- Month Three: January 2018
  - Implement

- Month Four: February
WE NEED YOU

R & D - Blockchain

Volunteers

Cyber Intelligence

Response

Incident
Our agenda is unashamedly ambitious; we want to be a world leader in cyber security.”

Ciaran Martin
CEO NCSC

£1.9 billion UK Government investment in Cyber by 2020
Thank you for listening

Any Questions?

Eamonn.keane@SBRCentre.co.uk

POLICE SCOTLAND