Tackling Cyber threats together

Sean O'Neil

Areas of discussion (in brief)

- What is Cyber Crime?
- Recent intelligence and current threats
- Advice on how to protect yourselves
- Ways you may choose to protect yourselves, with CBR, CisP, POC.

What is Cyber Crime?

The adopted definition of Cyber Crime is:

- *Cyber Dependent Crimes*, where a digital system is the target as well as the means of attack. These include attacks on computer systems to disrupt IT infrastructure, and stealing data over a network using malware (the purpose of the data theft is usually to commit further crime).

- *Cyber Enabled Crimes*. 'Existing' crimes that have been transformed in scale or form by their use of the Internet. The growth of the Internet has allowed these crimes to be carried out on an industrial scale.

- The use of the Internet to facilitate drug dealing, people smuggling and many other 'traditional' crime types.

BEDFORDSHIRE POLICE
Protecting People and Fighting Crime
Together

BEDFORDSHIRE POLICE
Cybercrime
Digital Forensics & Investigations Unit

Which of these is a cyber threat?

POTENTIALLY ALL OF THEM!

But what are some of the biggest threats?

- Insider Threat (theft/fraud/data breach)
- Malware by phishing attacks
- Data Breach
- DDoS
- Social Engineering leading to scams
- Theft/fraud by Customers or vendors.

Ultimately it depends on the business, how it is set up, the infrastructure and the policies and procedures, and protect mechanisms in place.

Does your BCP include no use of IT or loss of data!

And now for some good news!!

GCHQ reported in 2014 that in terms of Cyber Crime...

80% is easily preventable

Current Scams

Invoice emails – i.e. new vendors, changes to current vendors, Apple [little mix]

Vouchers -   Supermarkets, on line stores

Account updates – amazon, Sky, Virgin, Utilities.

Advice – any unsolicited emails. Do not press that link; simply delete. Go via normal website. Send to phishing email address for company

Microsoft/BT router/system faults – Dunstable case £4500

Advice – Do not engage,   go via normal website.

Mandate fraud – Bedford company lost £100K 3 weeks ago. 27 staff at risk. £1M in Luton in September.

Advice - Slow down, check via second source. Get copy of our advice.

Ransomware – suckers list

Advice - Plan with 2x back ups, have details of local IT repair company

Insider threat

- Theft/fraud by employee
- Data breach (increased threat when leaving – take to new employment, sell).
- Click the link on phishing emails

- Tactical advice
- NDA (visitors & employees)
- ICT group permissions
- Encrypt data at rest.
- account closure process.
- Training and advice to staff of Cyber security.

BEDFORDSHIRE POLICE
Protecting People and Fighting Crime
Together

BEDFORDSHIRE POLICE
Cybercrime
Digital Forensics & Investigations Unit

Mandate fraud / CEO fraud
Dodgey Sean

Fraudsters targeting senior Executives.

- Fraudsters target residential premises in affluent areas; letterboxes and waste bins that lack security & CCTV - to steal victims' mail, specifically banking documentation and personal correspondence.

- Identify senior executives of companies/organisations.

- Complete open source research to identify if suitable position to target (fb, twitter, LinkedIn)

- Conduct social engineering to gather information including family details.

- Visit business location!

- Carry out mandate and payment diversion fraud on the company.

- Tactical advice: Check mailbox regularly, assess where mail is deposited for vulnerabilities. Consider security measures. Dispose of confidential mail securely i.e. shredding. Place bins in locked location, consider CCTV coverage.

- To reduce social engineering consider what information you place on social networking sites regarding you, your home, and place of employment.

- Put in place company procedures to challenge/double check any attempt to

- change any payment details.

BEDFORDSHIRE POLICE
Protecting People and Fighting Crime
Together

BEDFORDSHIRE POLICE
Cybercrime
Digital Forensics & Investigations Unit

Ways you may choose to protect yourselves:

- **CBR –** Free service to all local businesses, organisations, charities, vulnerable people
- Offering a review of current practices
- Suggesting improvements to ICT/physical security
- Leading to greater ability to reach 'cyber essentials' accreditation - Minimum standard suggested for government contracts in the future.

- **CisP**
- **POC**

CiSP – Cyber Information Sharing Partnership
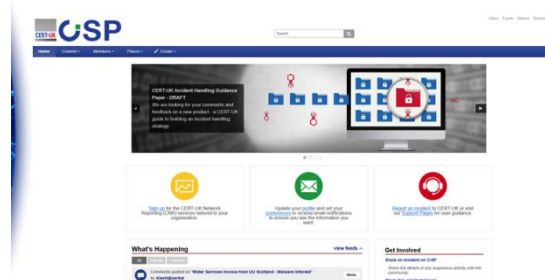
Let's Finish on five Simple Pieces of Advice...
'Bunch of fives'

Use strong passwords

A strong password is your first defence against hackers and cyber criminals.

Find out more

Install security software

Security software such as antivirus helps protect your devices from viruses and hackers.

Find out more

Download software updates

Software updates contain vital security upgrades which help keep your devices secure

Find out more

Screen clippings taken from www.cyberstreetwise.com

- Back up your data – at least twice - ensure it is not constantly connected to your server.

- Encrypt all data at rest on your server. I.e. spreadsheet with customer data, personal data. Details that you do not wish to loose. Most data loss reported is because data has not been encrypted.

Thank you!

Sean O'Neil
Cyber Security Advisor (2219)

Bedfordshire Police Headquarters,
Woburn Road, Kempston, Bedfordshire, MK43 9AX

(+44) 7720204358
sean.oneil@bedfordshire.pnn.police.uk

cyberprotect@bedfordshire.pnn.police.uk

Eventbrite 🔍 Search for events

Cyber threat awareness and guidance event for businesses in bedfordshire 2017. `LIVE`

Luton, United Kingdom | Putteridge Bury

Thursday, 2 February 2017 from 09:00 to 15:30 (GMT)

BEDFORDSHIRE POLICE
Protecting People and Fighting Crime
Together

BEDFORDSHIRE POLICE
Cybercrime
Digital Forensics & Investigations Unit