ITSUS CONSULTING

SECURE COMMUNICATIONS EXPERTLY DELIVERED

ITSUS CONSULTING

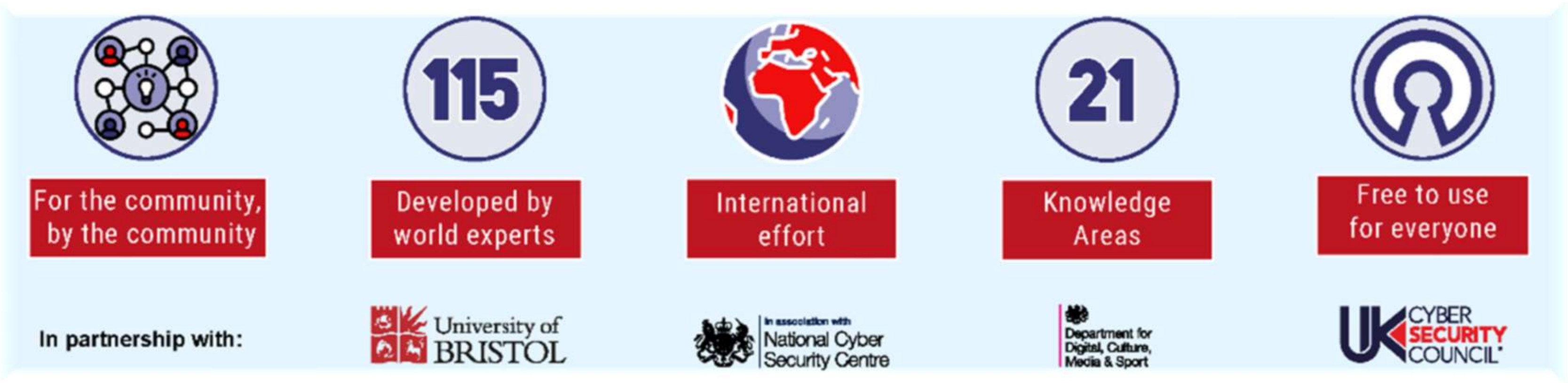
CyBOK

CyBOK Workshop for Local Authorities / Education

Thinking outside the (Cy)BoX

Dr Clare Johnson | Dr Jack Whitter-Jones | Andrew Johnson

CyBOK Overview:
What is CyBOK?

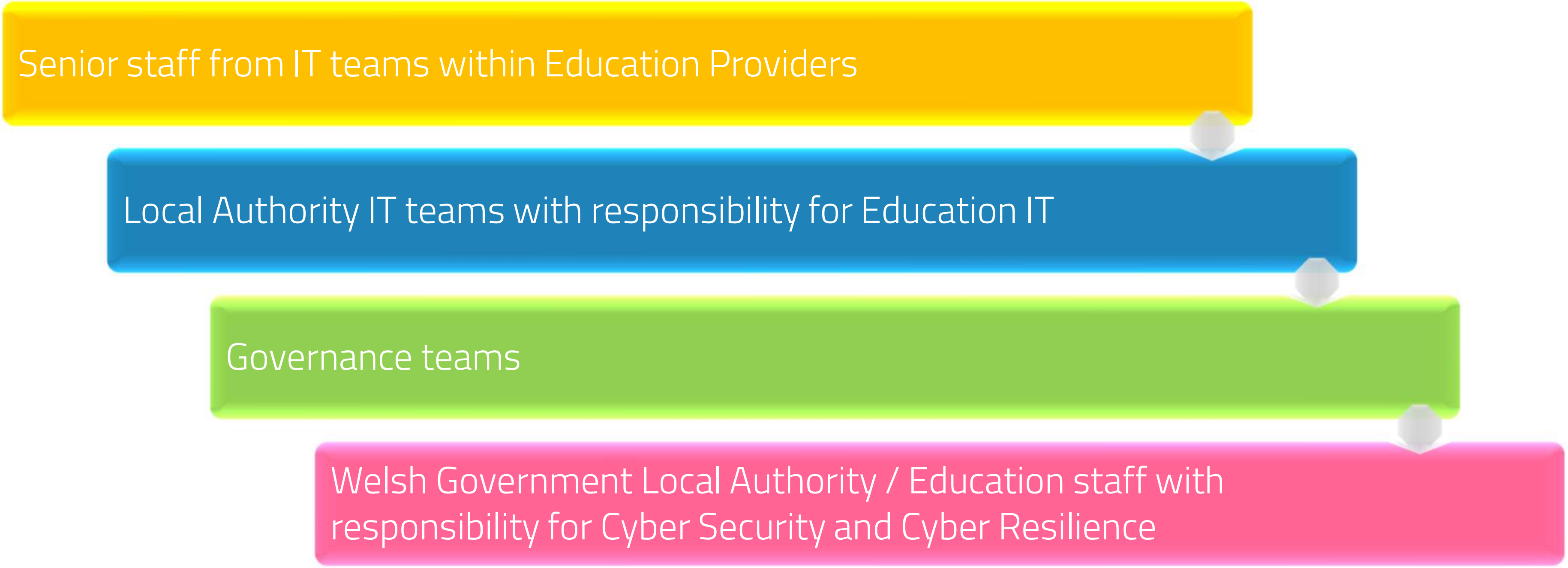

115
21
For the community, by the community
Developed by world experts
International effort
Knowledge Areas
Free to use for everyone
In partnership with:
University of BRISTOL
In association with National Cyber Security Centre
Department for Digital, Culture, Media & Sport
UK CYBER SECURITY COUNCIL

The CyBOK is a comprehensive body of knowledge for the Cyber Security sector. Designed to underpin education and professional training, it details 21 knowledge areas that encompass all aspects of cyber security, from Risk and Governance through to Cryptography and Cyber Physical Systems.

The CyBOK is well recognised in the educational sector and underpins a variety of degree programmes in UK universities including NCSC Certified Degrees. Its application to the wider community is less well established despite being of potentially significant benefit.

This project aims to explore CyBOK with established partners in the Education and Local Authority sectors, focusing on raising awareness of the resource, developing understanding of how it can best be applied to these sectors, and developing draft resources and recommendations for wider use within the sector.

CyBOK Overview:
Target audience



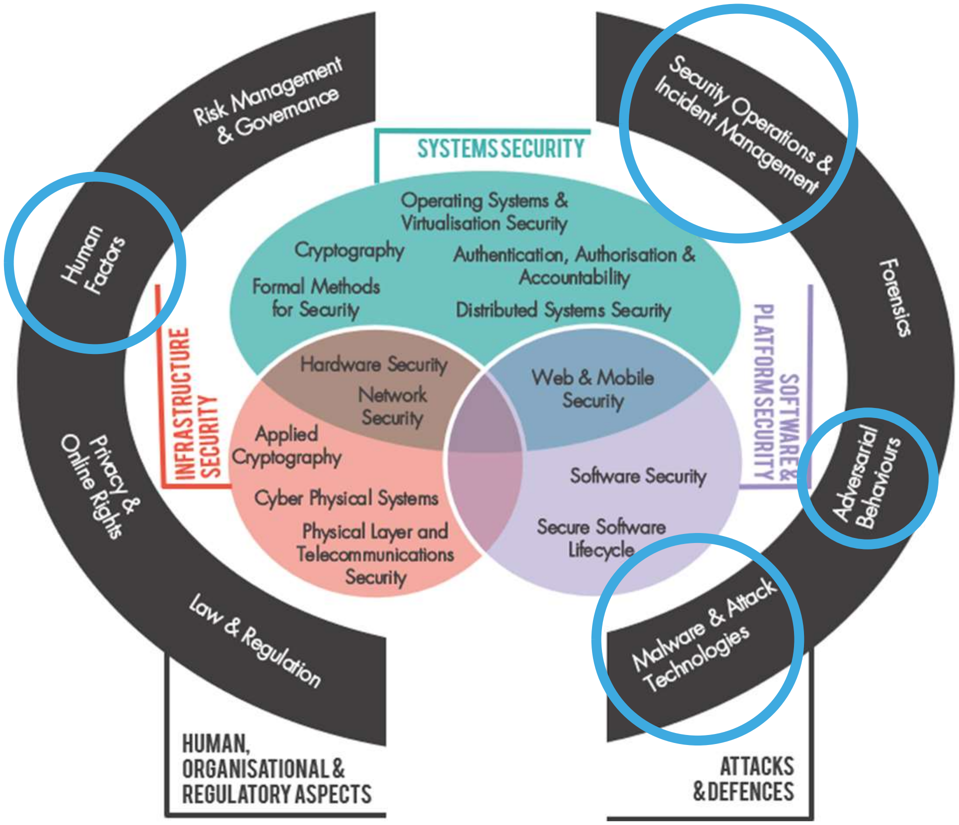
Senior staff from IT teams within Education Providers

Local Authority IT teams with responsibility for Education IT

Governance teams

Welsh Government Local Authority / Education staff with responsibility for Cyber Security and Cyber Resilience

CyBOK Overview: Knowledgebase Areas



Risk Management & Governance
Human Factors
Privacy & Online Rights
Law & Regulation
HUMAN, ORGANISATIONAL & REGULATORY ASPECTS
SYSTEMS SECURITY
Operating Systems & Virtualisation Security
Cryptography
Authentication, Authorisation & Accountability
Formal Methods for Security
Distributed Systems Security
INFRASTRUCTURE SECURITY
Hardware Security
Network Security
Applied Cryptography
Cyber Physical Systems
Physical Layer and Telecommunications Security
SOFTWARE & PLATFORM SECURITY
Web & Mobile Security
Software Security
Secure Software Lifecycle
Security Operations & Incident Management
Forensics
Adversarial Behaviours
Malware & Attack Technologies
ATTACKS & DEFENCES

Scenario 1.1: Adversary – Helen Back (IT Analyst)

KA: https://www.cybok.org/media/downloads/Adversarial_Behaviours_v1.0.1.pdf

Helen Back is an IT Analyst who has worked for Mordor District Council for 3 years. During her employment, Helen has had multiple disagreements with her management team, colleagues and has had several altercations with management regarding her working environment, her daily workloads, and her personal development. During her last personal development review, Helen was not offered a pay increase and was not offered a promotion internally to become a senior IT analyst. In addition, there are internal ‘whispers’ of redundancies within the IT Support department due to an internal restructure.

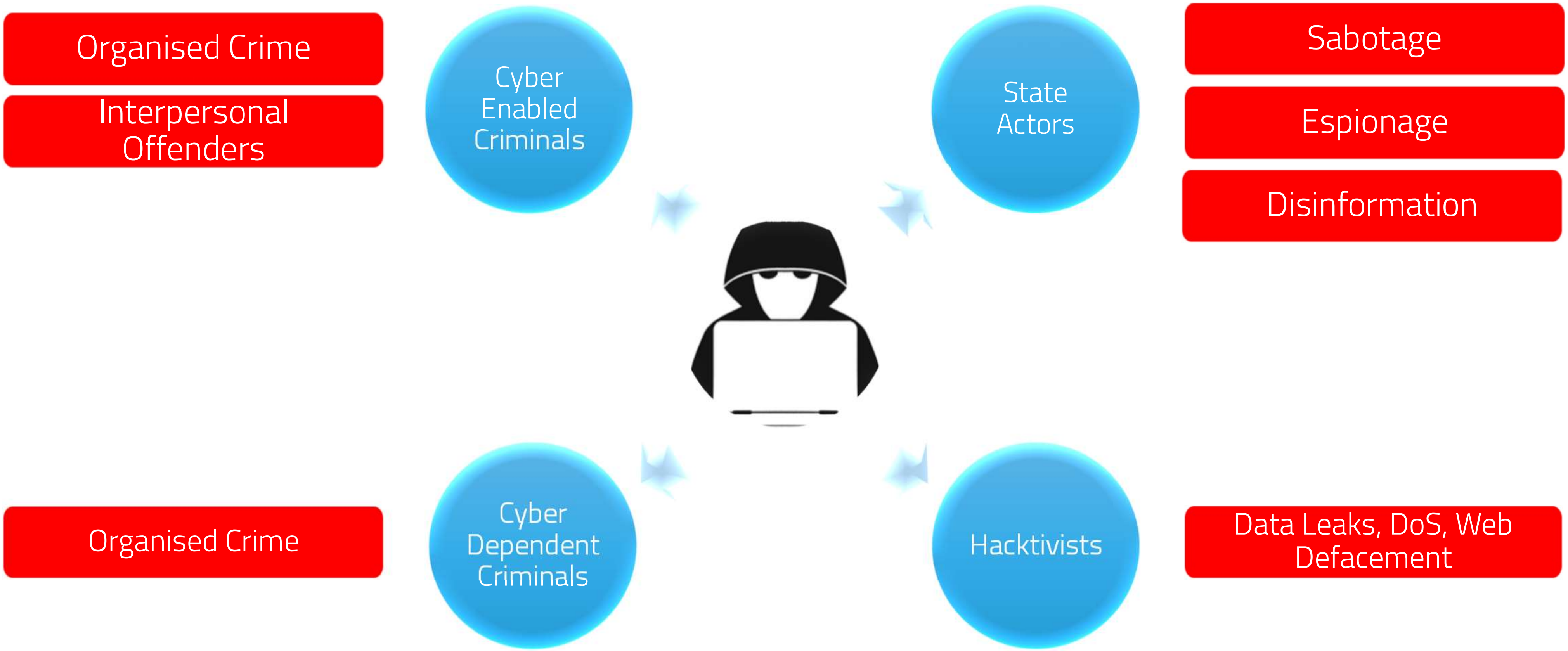
Helen Back is an example of a disgruntled employee. She has given in her notice, and on the day she leaves the office she plants a malicious ‘leaving present’ - The ‘Rubber Ducky’ USB.

A rubber ducky USB will emulate a user's keyboard when plugged into a USB port and can be used to execute commands and execute malware. In this context , Helen has uploaded an executable ransomware onto the USB disguised as a pdf file entitled ‘Redundancies 2023’. The USB has been labelled as ‘Redundancies 2023’ and Helen has left it in the IT Support department’s kitchen just before she leaves for good. Helen is also aware that Evan takes an early lunch break at 12:00.

Discussion Point – Why do you think Helen is behaving in this manner? What security processes should be in place to protect the organisation from potential adversaries such as Helen?

KA – Adversarial Behaviours: Characteristics of Adversaries: Cyber-Dependent/Enabled Crime

https://www.cybok.org/media/downloads/Adversarial_Behaviours_v1.0.1.pdf



Organised Crime

Interpersonal Offenders

Cyber Enabled Criminals

State Actors

Sabotage

Espionage

Disinformation

Organised Crime

Cyber Dependent Criminals

Hacktivists

Data Leaks, DoS, Web Defacement

Scenario 1.2: Human Factor – Evan Lee – IT Support Analyst

KA: https://www.cybok.org/media/downloads/Human_Factors_v1.0.1.pdf

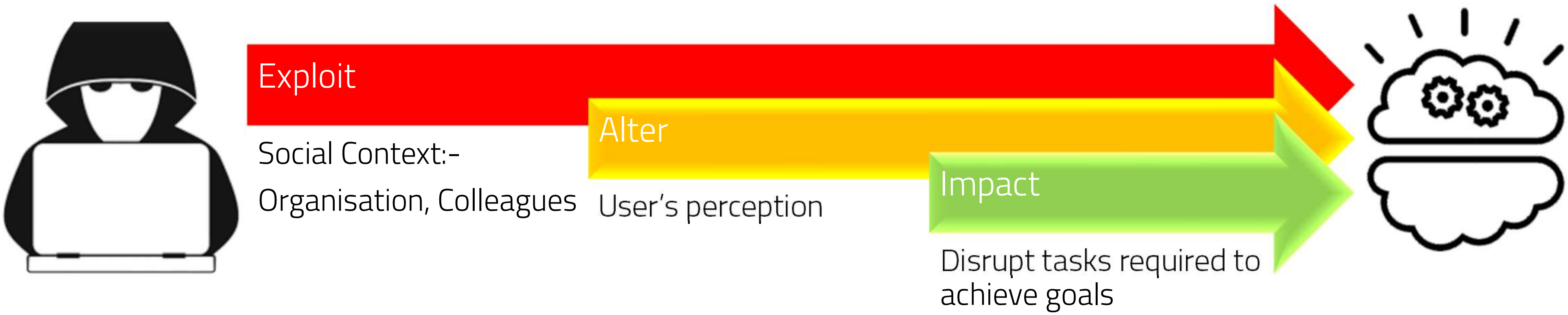
Evan Lee is the newest member of the IT Support team at Mordor District Council. Evan has only been with the council for 6 months and has recently bought a house as he has passed his probation. However, talk amongst the department colleagues regarding upcoming redundancies has left Evan worried that he may lose his job as he is the newest member of the team.

Evan is the unfortunate victim in this scenario: on his lunch break he finds the Rubber Ducky USB in the kitchen labelled 'Redundancies 2023', curiosity gets the better of him and he takes the USB.

Discussion Point – What factors do you think are contributing to Evan's behaviour?

KA – Human Factors:
Understanding Human Behaviour in Security

https://www.cybok.org/media/downloads/Human_Factors_v1.0.1.pdf



Exploit

Social Context:-

Organisation, Colleagues

Alter

User's perception

Impact

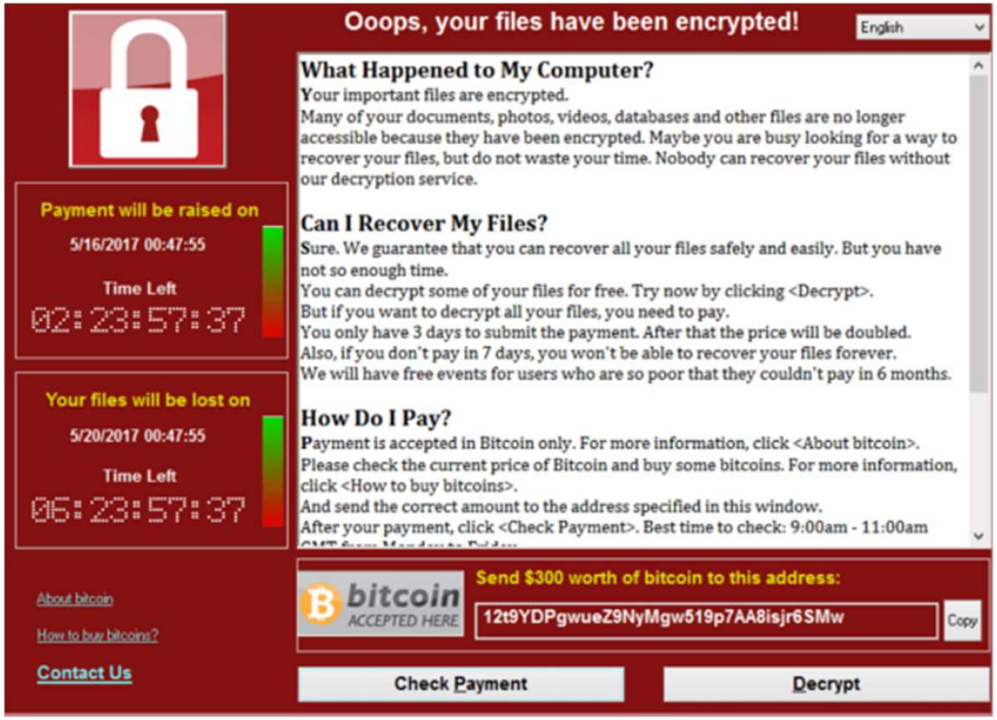
Disrupt tasks required to achieve goals

Scenario 1.3: The ransomware

KA: https://www.cybok.org/media/downloads/Malware_Attack_Technologies_v1.0.1.pdf

Evan inserts the USB into his PC and sees the pdf entitled ‘Redundancies-2023’. Evan double clicks the file to open it up and the file disappears.

Evan is confronted by a ransomware message:



Ooops, your files have been encrypted!

What Happened to My Computer?

Your important files are encrypted.

Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

Payment will be raised on
5/16/2017 00:47:55
Time Left
02:23:57:37

Your files will be lost on
5/20/2017 00:47:55
Time Left
06:23:57:37

Send $300 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

Scenario 1.3: The ransomware

KA: https://www.cybok.org/media/downloads/Malware_Attack_Technologies_v1.0.1.pdf

The ransomware is malicious software that encrypts a user's files making them unavailable. It is a security breach as it has broken the CIA (Confidentiality, Integrity and Availability) triad by making files unavailable, which has affected the integrity and availability of the data.

The ransomware has also gained 'persistence' on Evan's machine, by creating its own set of Windows keys inside the Windows registry. Evan tries several times to reboot his PC but the pop up remains.

Caroline Sweet is a colleague of Evan's, and the ransomware has spread to her machine. She immediately reports this to the security team.

Discussion point – Discuss the actions of Evan and Caroline. What immediate action should either of them have taken?

KA – Malware & Attack Technologies: Malware Activities – The Cyber Kill Chain

https://www.cybok.org/media/downloads/Malware_Attack_Technologies_v1.0.1.pdf

Reconnaissance	Harvesting email addresses, identifying vulnerable computers and accounts, etc
Weaponization	Designing exploits into a deliverable payload.
Delivery	Delivering the exploit payload to a victim via email, Web download, etc.
Exploitation	Exploiting a vulnerability and executing malicious code on the victim’s system.
Installation	Installing (additional) malware on the victim’s system.
Command & Control	Establishing a command and control channel for attackers to remotely commandeer the victim’s system.
Actions on Objectives	Carrying out malicious activities on the victim’s system and network.

Scenario 1.4: Incident response

KA: https://www.cybok.org/media/downloads/Security_Operations_Incident_Management_v1.0.2.pdf

Seymour Johnson works in the Security department of Mordor District council as a security analyst.

After receiving a telephone call from Caroline, his first action is to follow incident reporting procedure by creating an incident at a Level 1 priority on the internal incident reporting system, and reporting this to senior managers by email. He then removes every machine in the IT Support department from the network.

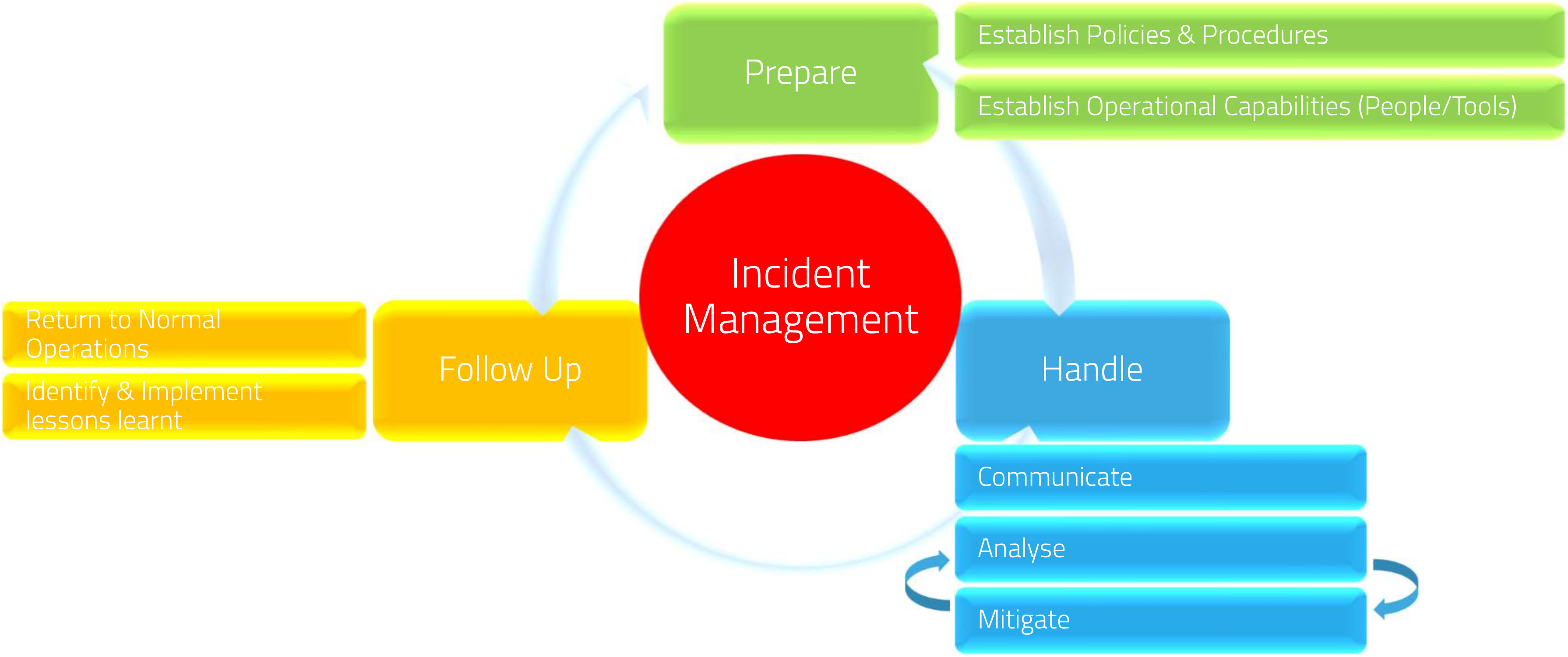
However, several other users across other departments, finance and administration have also had their machines infected.

After receiving further calls from other colleagues across the corporate estate, the decision is made to take down the corporate network.

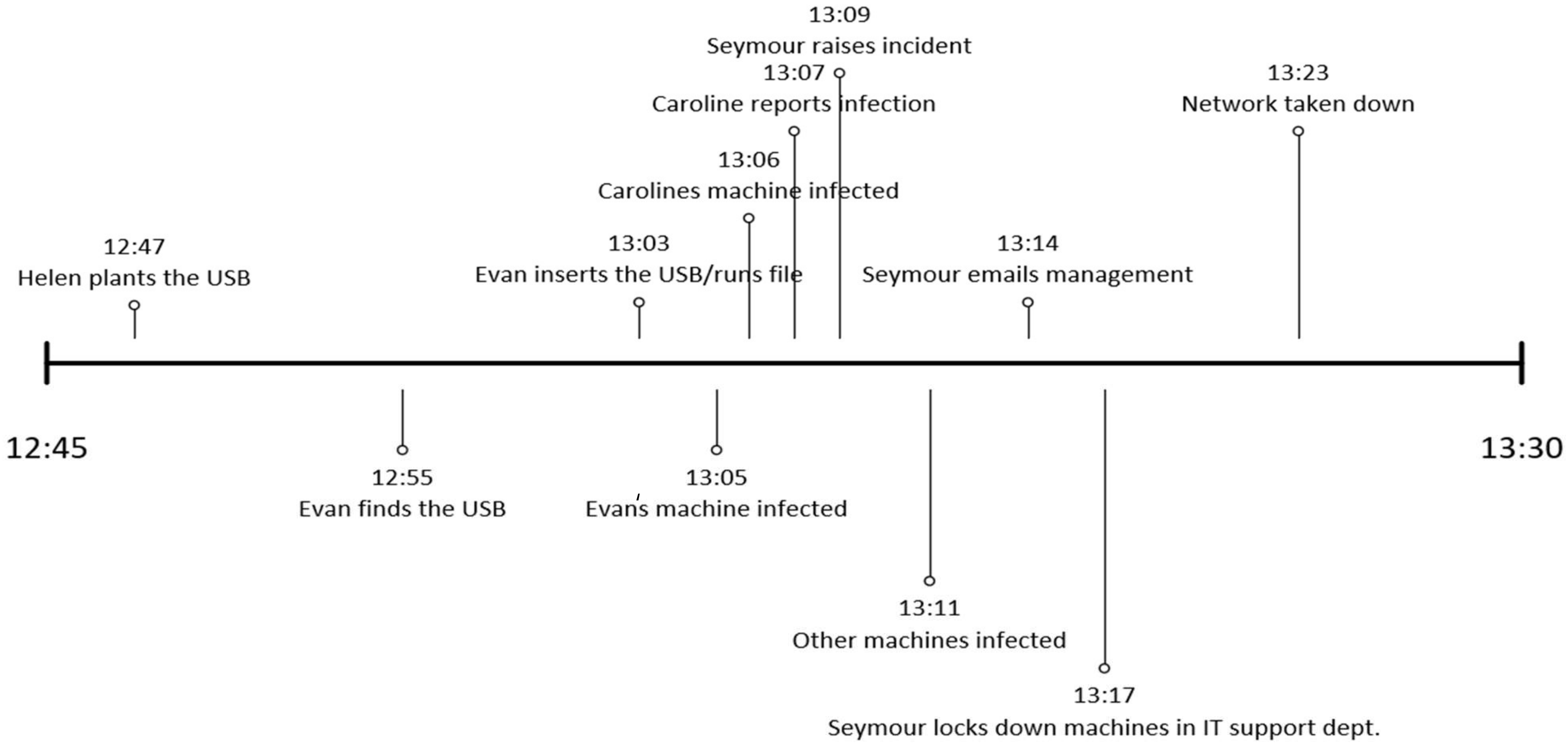
Discussion – Could Seymour have taken more immediate remediation to prevent the spread of the ransomware? Discuss the incident reporting procedures in place in your organisation. What security solutions do you think could have prevented the malware infection and propagation?

KA - Security Operations and Management: Incident Management

https://www.cybok.org/media/downloads/Security_Operations_Incident_Management_v1.0.2.pdf


Prepare
Establish Policies & Procedures
Establish Operational Capabilities (People/Tools)
Incident Management
Handle
Communicate
Analyse
Mitigate
Follow Up
Return to Normal Operations
Identify & Implement lessons learnt

Scenario 1: Timeline



12:45

12:47
Helen plants the USB

12:55
Evan finds the USB

13:03
Evan inserts the USB/runs file

13:05
Evan's machine infected

13:06
Carolines machine infected

13:07
Caroline reports infection

13:09
Seymour raises incident

13:11
Other machines infected

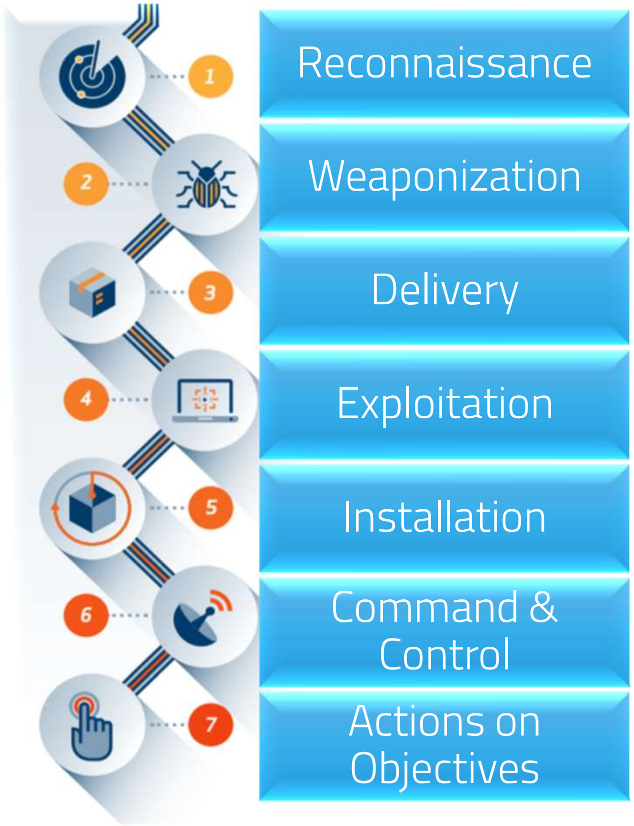
13:14
Seymour emails management

13:17
Seymour locks down machines in IT support dept.

13:23
Network taken down

13:30

Scenario Summary: The Cyber Kill Chain Context – Complete the sections in white with the actions taken by Helen and Evan for each of the CKC steps below.



Reconnaissance

Weaponization

Delivery

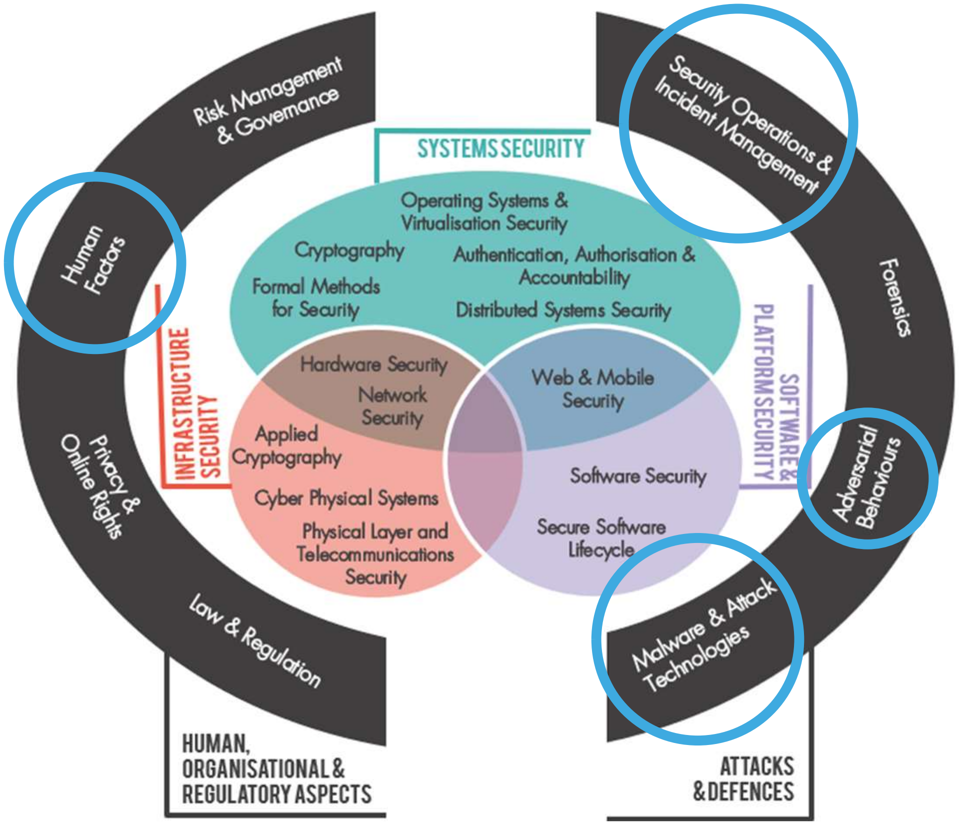
Exploitation

Installation

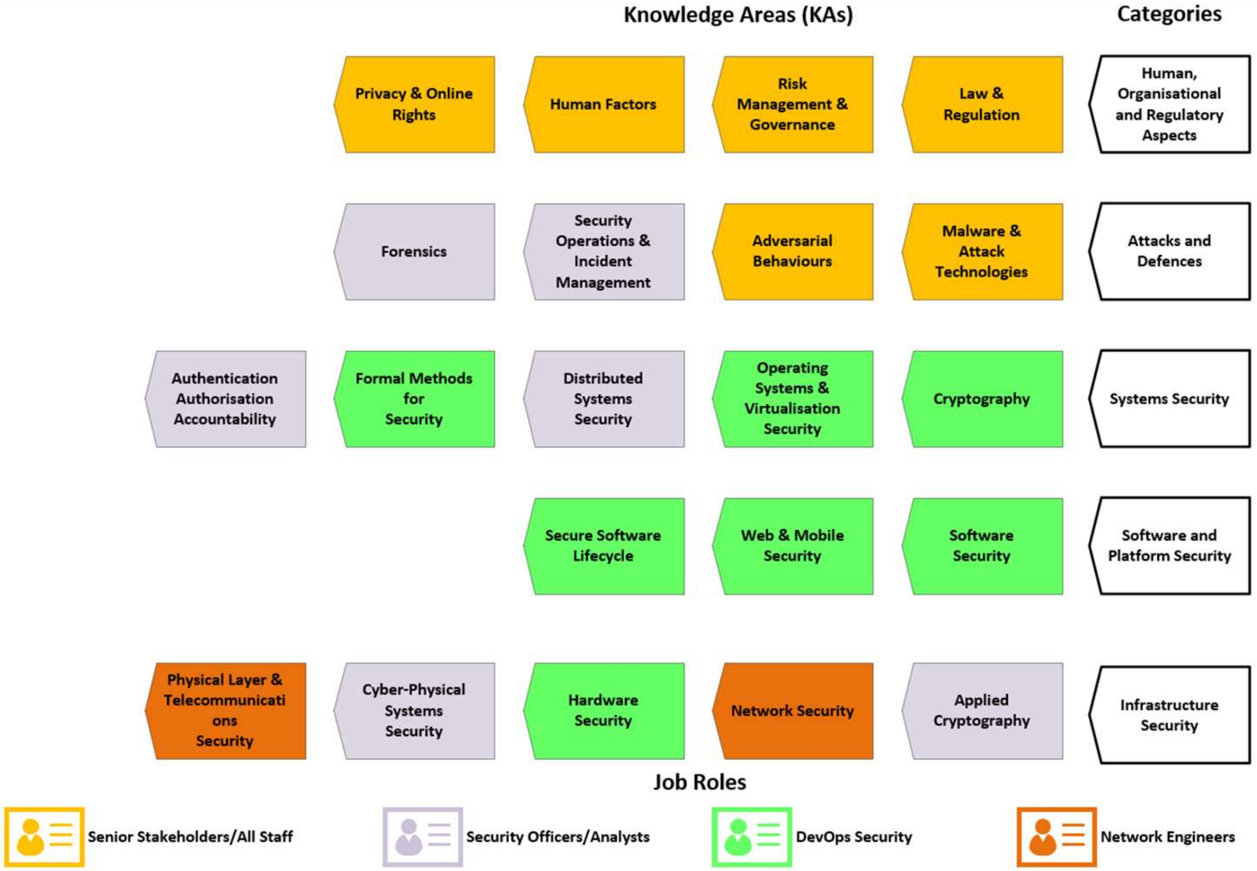
Command & Control

Actions on Objectives

CyBOK Overview: Knowledgebase Areas


Risk Management & Governance
Human Factors
Privacy & Online Rights
Law & Regulation
HUMAN, ORGANISATIONAL & REGULATORY ASPECTS
SYSTEMS SECURITY
Operating Systems & Virtualisation Security
Cryptography
Authentication, Authorisation & Accountability
Formal Methods for Security
Distributed Systems Security
INFRASTRUCTURE SECURITY
Hardware Security
Network Security
Applied Cryptography
Cyber Physical Systems
Physical Layer and Telecommunications Security
SOFTWARE & PLATFORM SECURITY
Web & Mobile Security
Software Security
Secure Software Lifecycle
Security Operations & Incident Management
Forensics
Adversarial Behaviours
Malware & Attack Technologies
ATTACKS & DEFENCES

Knowledge Areas (KAs) Mapping to Job Roles



		Knowledge Areas (KAs)				Categories
	🟨 Privacy & Online Rights	🟨 Human Factors	🟨 Risk Management & Governance	🟨 Law & Regulation		Human, Organisational and Regulatory Aspects
	🟪 Forensics	🟪 Security Operations & Incident Management	🟨 Adversarial Behaviours	🟨 Malware & Attack Technologies		Attacks and Defences
🟪 Authentication Authorisation Accountability	🟩 Formal Methods for Security	🟪 Distributed Systems Security	🟩 Operating Systems & Virtualisation Security	🟩 Cryptography		Systems Security
		🟩 Secure Software Lifecycle	🟩 Web & Mobile Security	🟩 Software Security		Software and Platform Security
🟧 Physical Layer & Telecommunications Security	🟪 Cyber-Physical Systems Security	🟩 Hardware Security	🟧 Network Security	🟪 Applied Cryptography		Infrastructure Security

Job Roles

🟨 Senior Stakeholders/All Staff

🟪 Security Officers/Analysts

🟩 DevOps Security

🟧 Network Engineers

What Next?

This workshop has been the first phase of the planned deliverable to explore CyBOK with established partners in the Education and Local Authority sectors. We have focused on only four of the KAs represented in the CyBOK knowledge base. We are planning to deliver further phases delivering workshops based around some of the other KAs. Your feedback on this workshop is greatly appreciated, and will steer our decisions on other KAs to deliver on in the future.

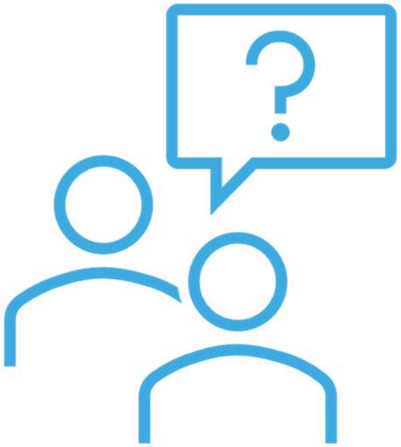
Resources

CyBOK Home Page - https://www.cybok.org/

CyBOK KAs - https://www.cybok.org/knowledgebase1_1/

THANK YOU FOR ATTENDING!!

Any Further Questions?



Our Expertise

We have experience working with academia to developing degree programmes that align with CyBOK, and certified by the NCSC.

Through our work in the defence section, we have a strong background in secure communications and a thorough understanding the importance of cyber security awareness.

We have existing relationships with Local Authorities responsible for education networks and Welsh Government Education teams.

CONTACT US

ITSUS Consulting
4 Earlswood Road, Llanishen, Cardiff CF14 5GH

Phone/Fax
T: 02920 003 170   F: 02920 007 062

Email
sales@itsusconsulting.com