What do we really mean by "Understanding Cyber Security"

Dr. Phil Legg

MSc Cyber Security Programme Lead

Senior Lecturer in Computer Science

June 2018

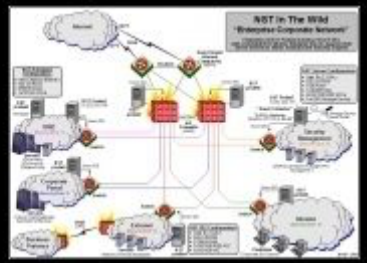
UWE Bristol | University of the West of England

Cyber Security

What my friends think I do.

What my mom thinks I do.

What society thinks I do.



What my boss thinks I do.

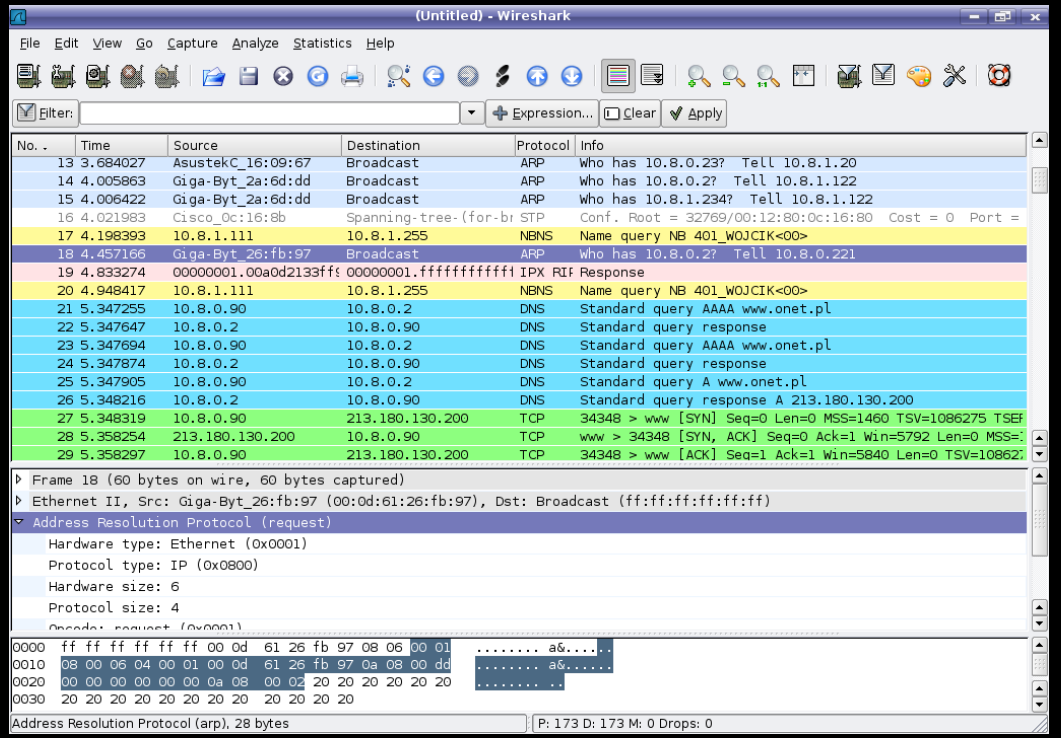
What I think I do.

What I actually do.

UWE Bristol | University of the West of England

“Typical” Cyber Security

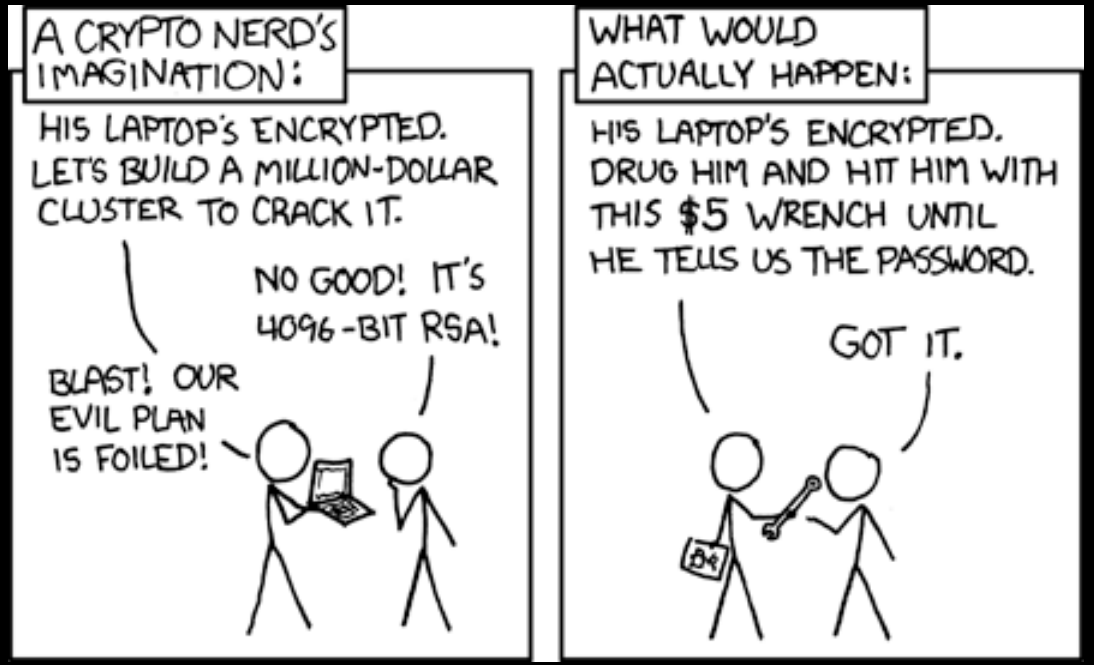
- Network traffic analysis
- Computer forensics
- Vulnerability assessment (Penetration testing)
- Risk management



UWE Bristol University of the West of England

Anything else?

- Human factors / Social Engineering
- Business Operations / Environmental Factors / Risk Management
- Cyber Security requires us to look beyond *only* technical security



Understanding Device Communications

- Today the world is full of "computers"
  - Smartphones,
  - "Smart " speakers
  - "Smart" fridges…
- If it communicates via the Internet it can potentially be compromised…

UWE Bristol | University of the West of England

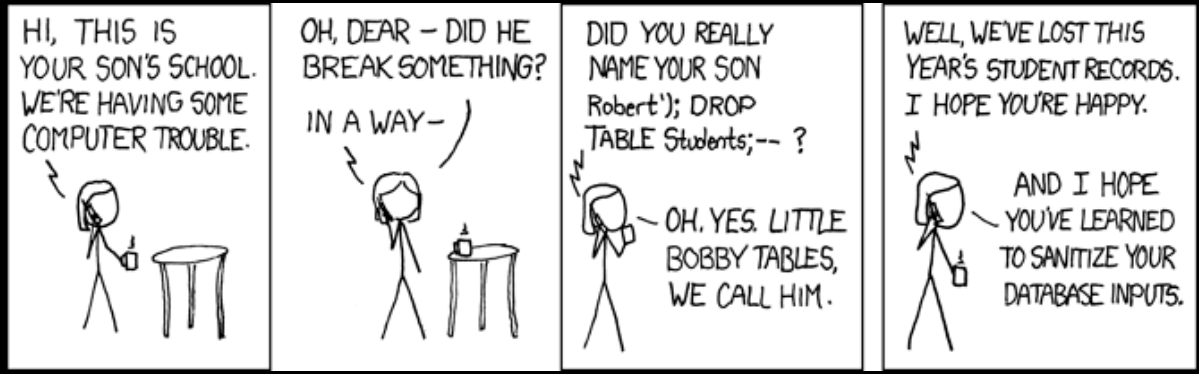
Understanding Device Communications

- OSI (Open System Interconnection) 7 Layer Model
- Essentially – how one application talks to another across a network
- If we want secure applications, we need all layers below to be secure also

Layer	Function	Example
Application (7)	Services that are used with end user applications	SMTP,
Presentation (6)	Formats the data so that it can be viewed by the user Encrypt and decrypt	JPG, GIF, HTTPS, SSL, TLS
Session (5)	Establishes/ends connections between two hosts	NetBIOS, PPTP
Transport (4)	Responsible for the transport protocol and error handling	TCP, UDP
Network (3)	Reads the IP address form the packet.	Routers, Layer 3 Switches
Data Link (2)	Reads the MAC address from the data packet	Switches
Physical (1)	Send data on to the physical wire.	Hubs, NICS, Cable

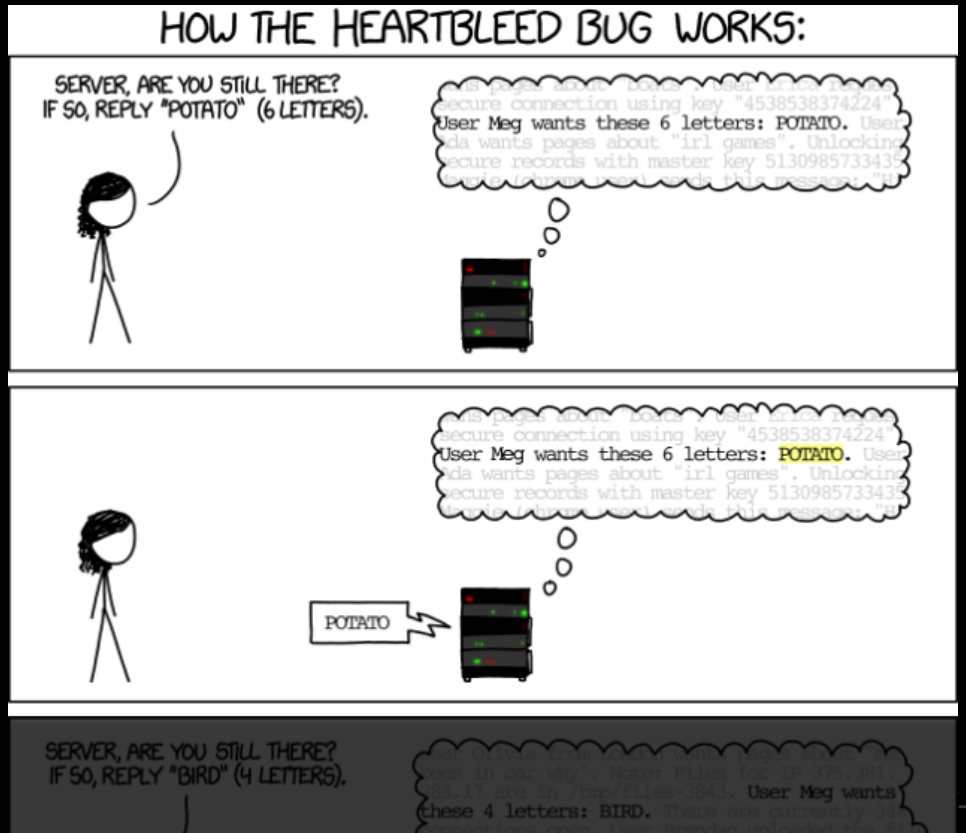
Understanding Software

- How can we develop secure software?
- What vulnerabilities may exist in poor coding?
- How can we "catch" unexpected user input?



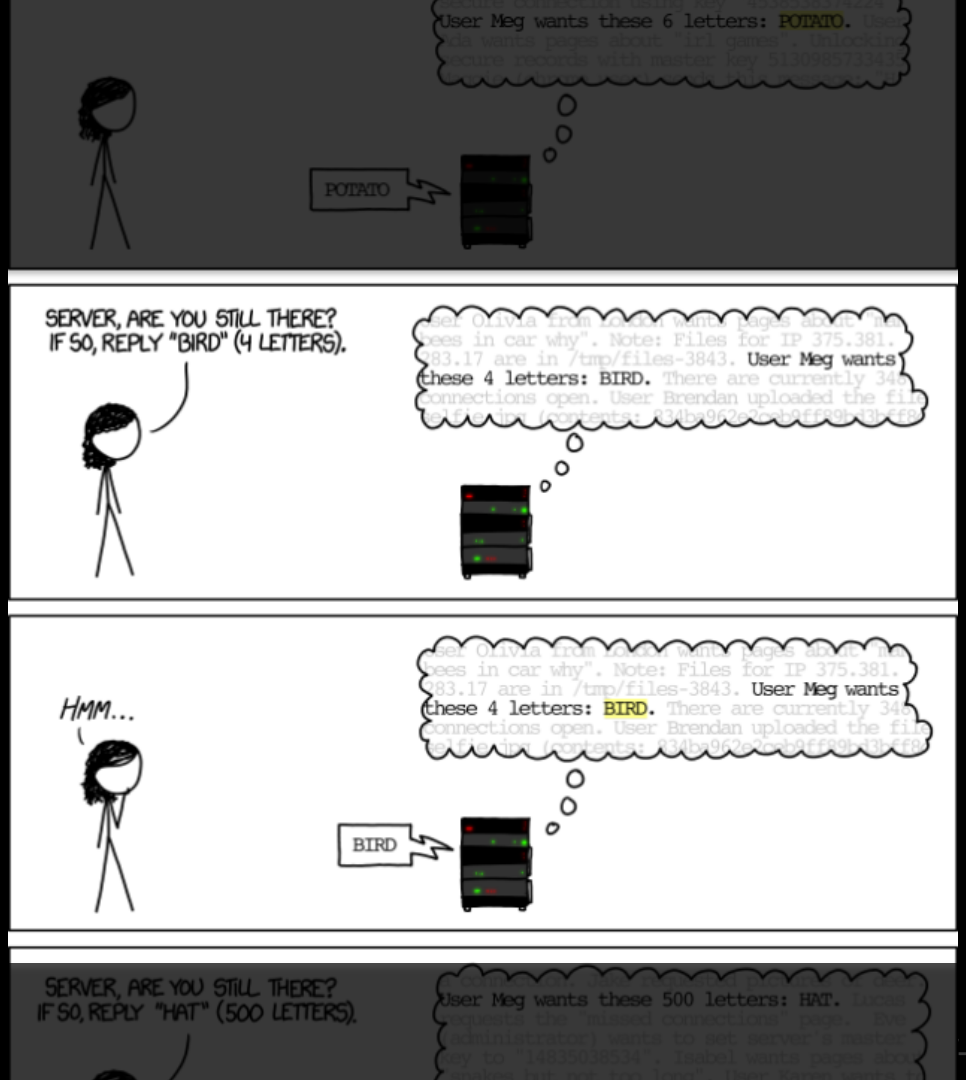
Heartbleed

- Heartbleed – web vulnerability in OpenSSL cryptography library, used in Transport Layer Security (TLS).
- Discovered in 2014, at the time around 17% of Internet's sercure servers were vulnerable – allowing theft of keys, cookies, and passwords.



Heartbleed

- Heartbleed – web vulnerability in OpenSSL cryptography library, used in Transport Layer Security (TLS).
- Discovered in 2014, at the time around 17% of Internet's sercure servers were vulnerable – allowing theft of keys, cookies, and passwords.



Heartbleed

- Heartbleed – web vulnerability in OpenSSL cryptography library, used in Transport Layer Security (TLS).
- Discovered in 2014, at the time around 17% of Internet's sercure servers were vulnerable – allowing theft of keys, cookies, and passwords.

https://en.wikipedia.org/wiki/Heartbleed
https://gizmodo.com/this-cartoon-is-the-simplest-explanation-of-

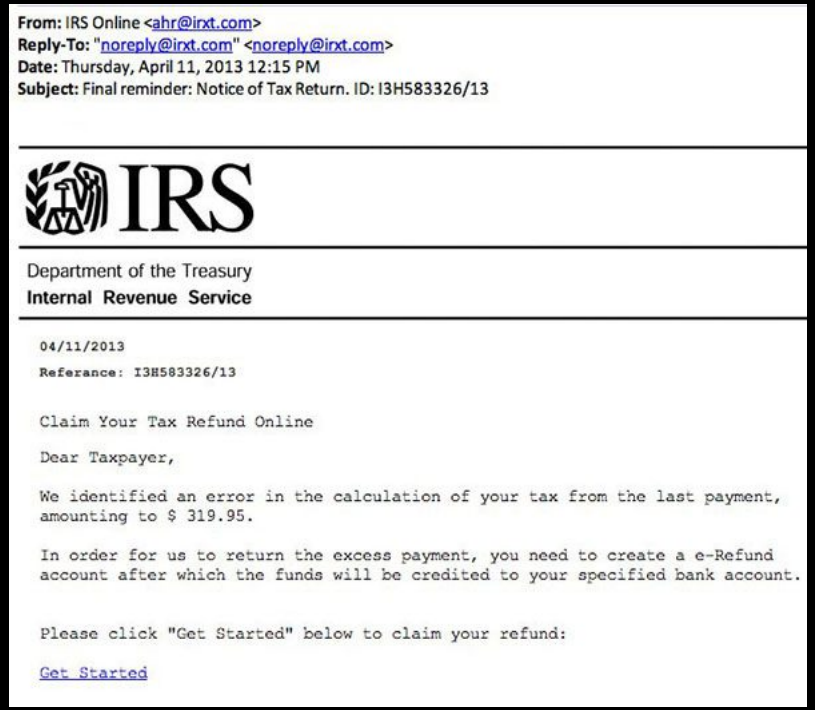
Understanding People

- What motivates cyber attacks?
- Can we learn about the people who carry out attacks?
- Can we learn about the people who are susceptible to attack?
- Social Engineering attacks.
- Spear phishing e-mail attacks.
- Insider threat attacks.

Understanding People

- Phishing e-mails – generic content that aims to fool victims.

- Spear phising e-mails – targeted attacks via phishing
  - May know personal details from social media / employer websites / professional sites (e.g. LinkedIn)
  - **Extremely effective!**



From: IRS Online <ahr@irxt.com>
Reply-To: "noreply@irxt.com" <noreply@irxt.com>
Date: Thursday, April 11, 2013 12:15 PM
Subject: Final reminder: Notice of Tax Return. ID: I3H583326/13

IRS

Department of the Treasury
Internal Revenue Service

04/11/2013

Referance: I3H583326/13

Claim Your Tax Refund Online

Dear Taxpayer,

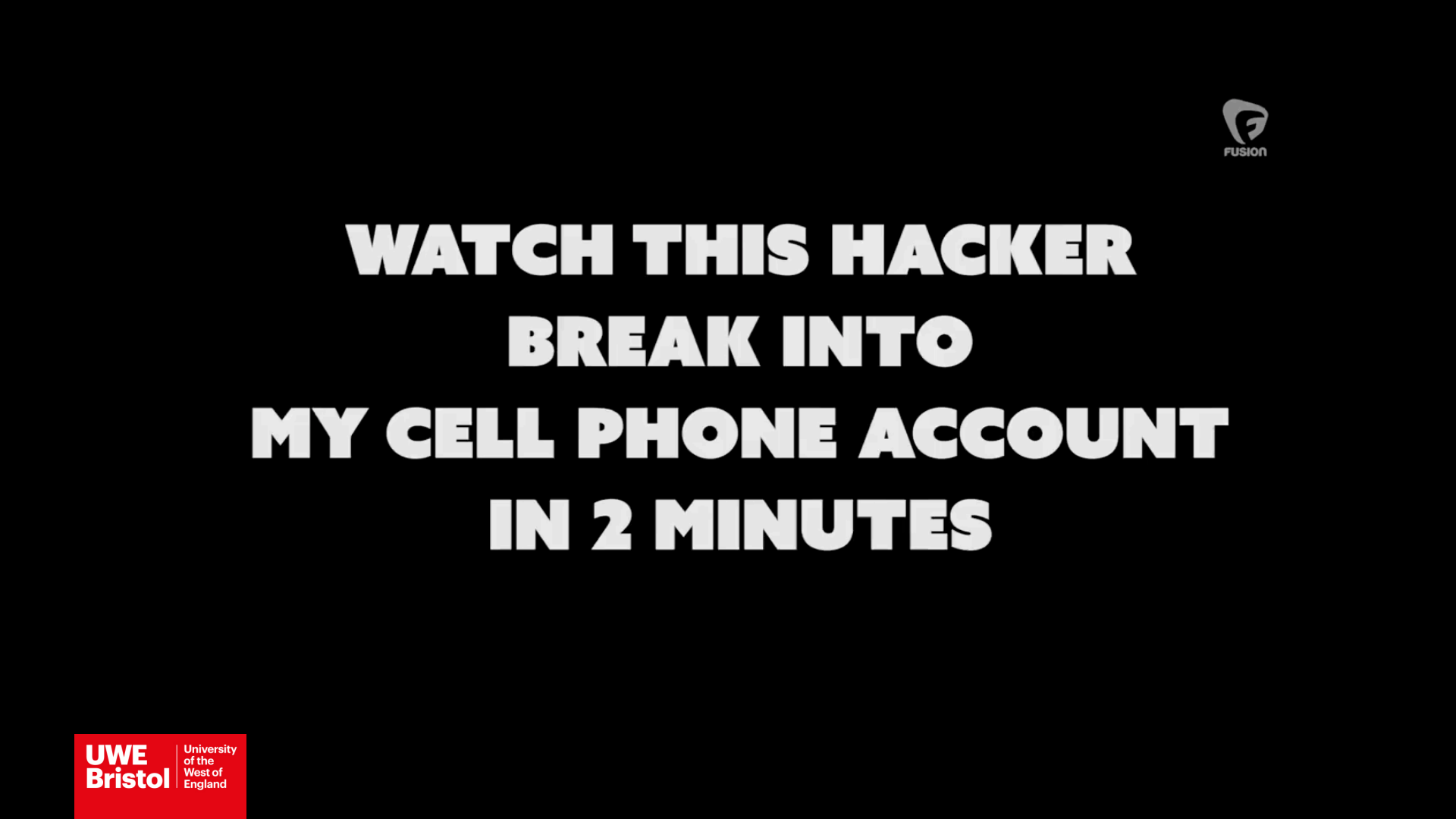
We identified an error in the calculation of your tax from the last payment, amounting to $ 319.95.

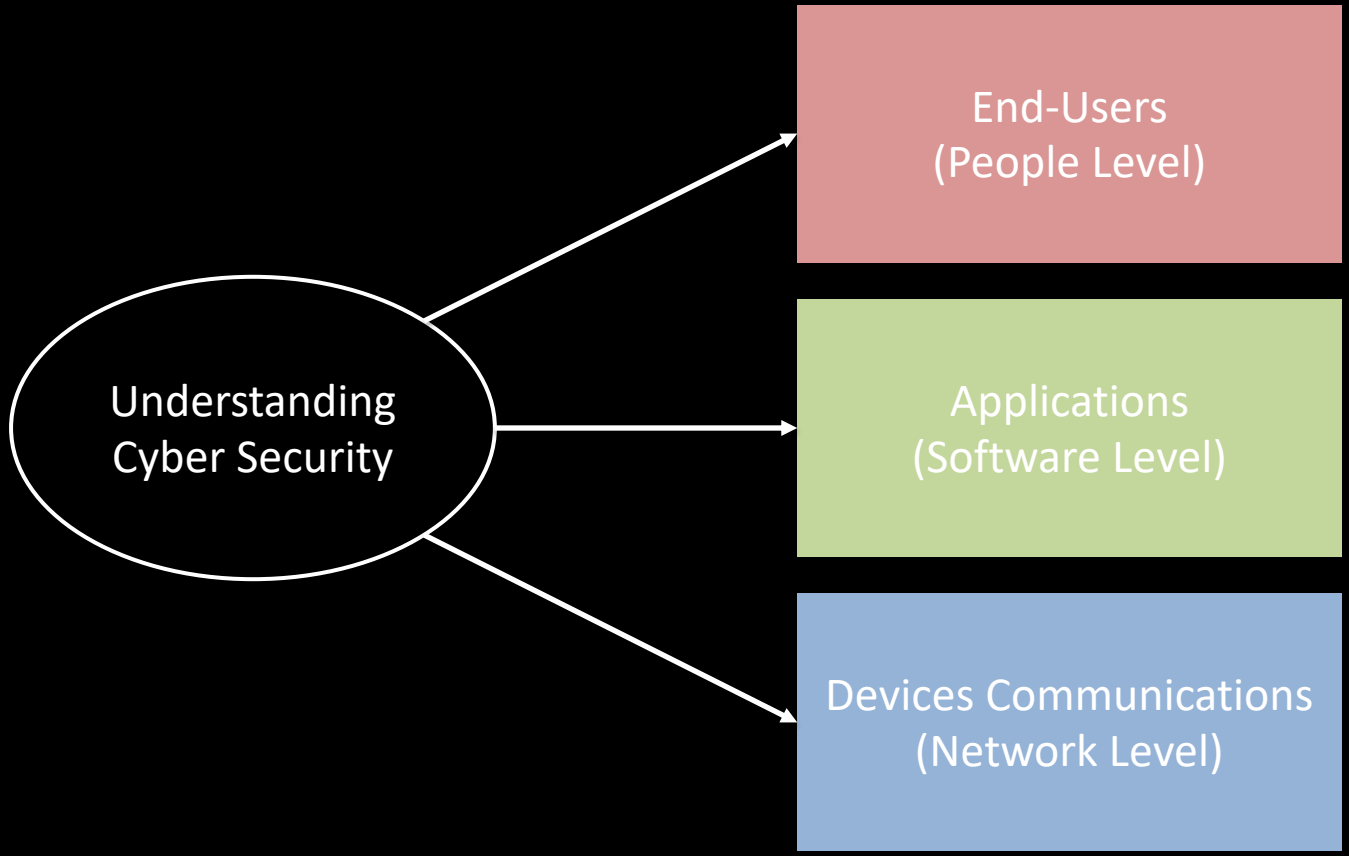
In order for us to return the excess payment, you need to create a e-Refund account after which the funds will be credited to your specified bank account.

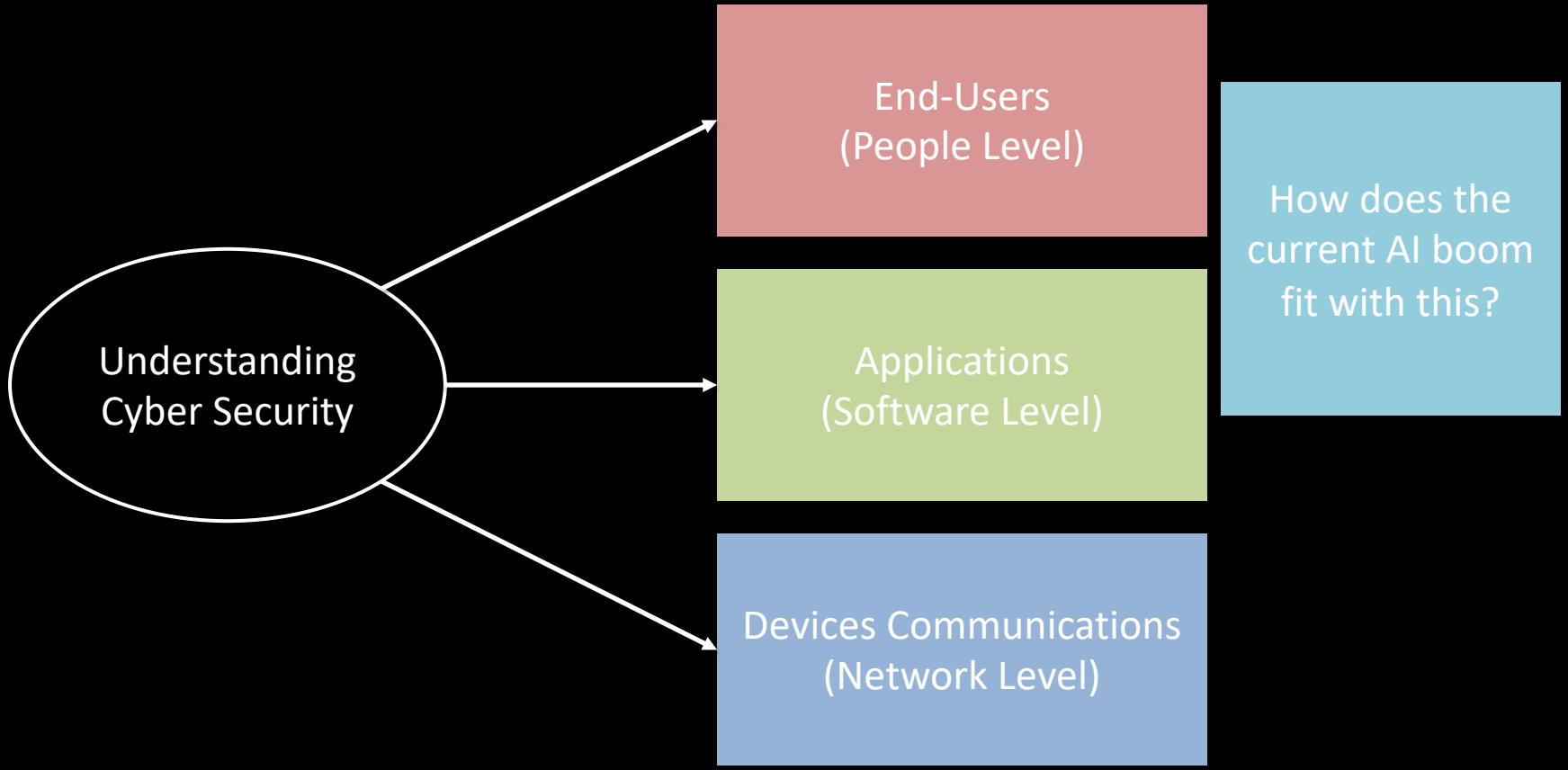
Please click "Get Started" below to claim your refund:

Get Started

UWE Bristol | University of the West of England





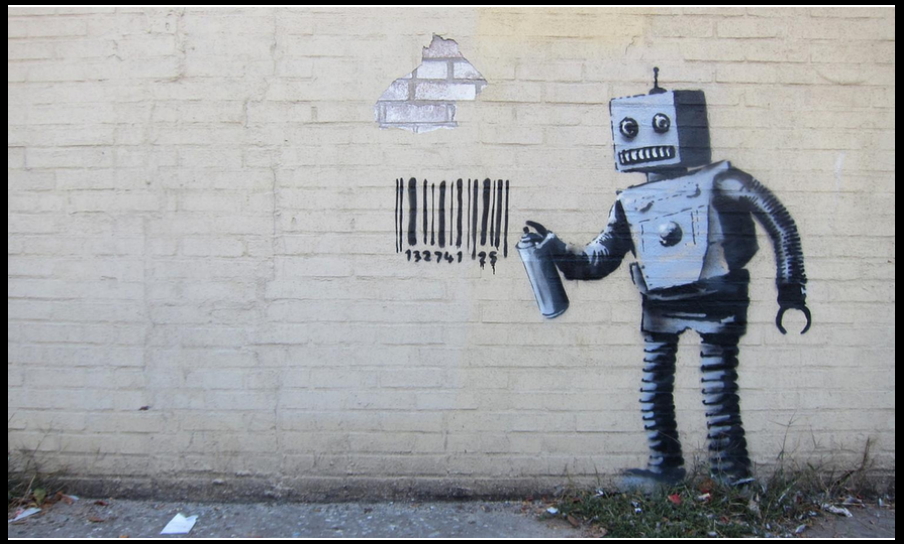

Understanding Cyber Security
End-Users (People Level)
Applications (Software Level)
Devices Communications (Network Level)
How does the current AI boom fit with this?

Understanding AI and Data

- What are the limitations of Machine Learning and AI?
- How may an adversary exploit AI?

- How can data samples be manipulated?
- How can ‘features’ be compromised?

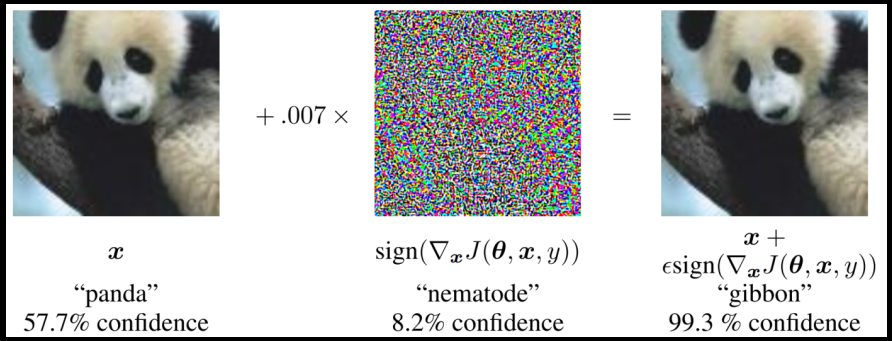
- How can/should humans oversee machine decisions?



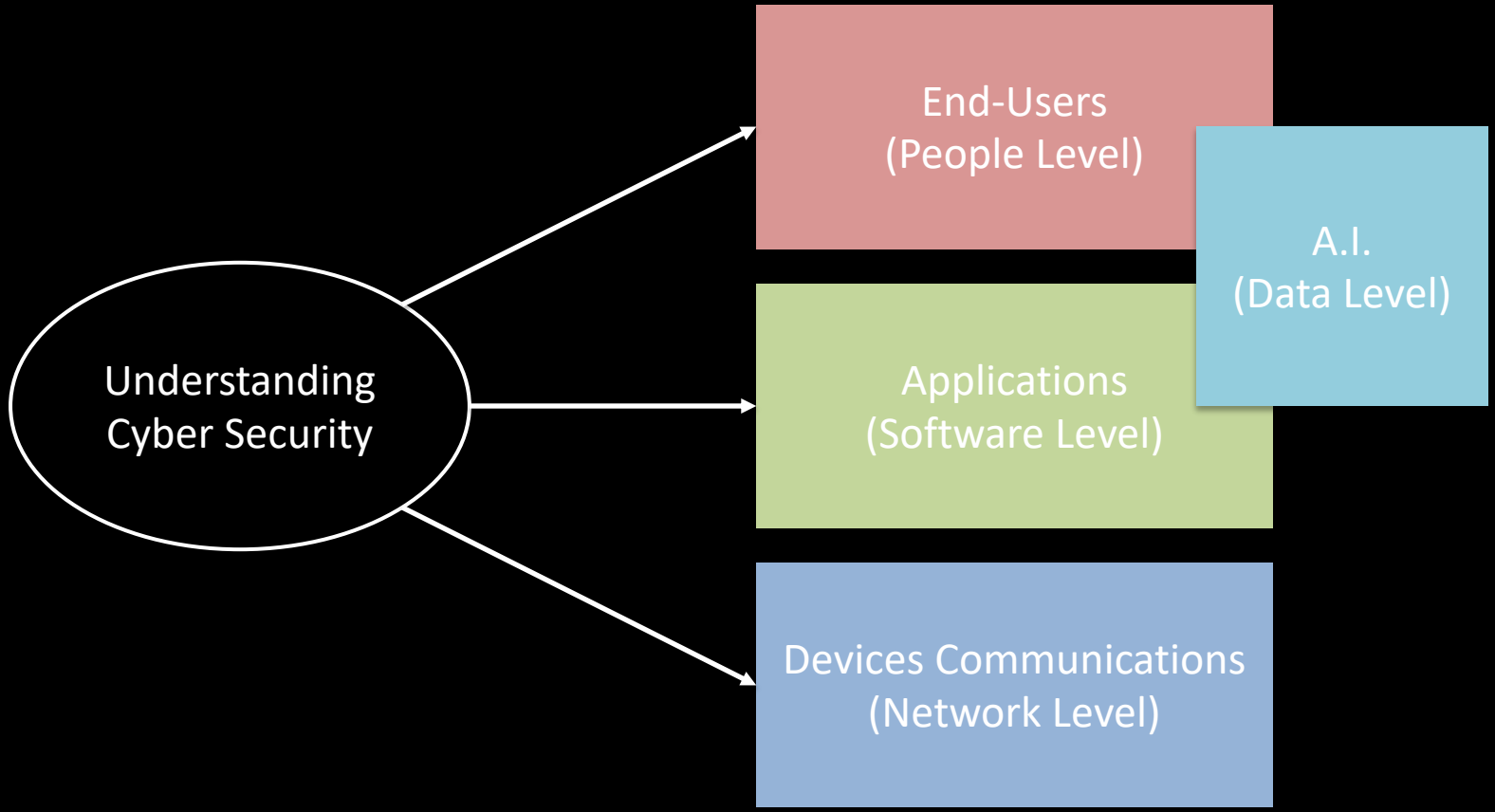
UWE Bristol | University of the West of England

Understanding AI and Data

- Hot topic in research currently
- "Adversarial learning" – the ability to learn how to corrupt a trained machine learning algorithm
- Many examples for image classification (e.g., panda / gibbon)
  - What if we can fool security systems in a similar fashion?



UWE Bristol | University of the West of England



Professional vs Personal

- Internet usage is ubiquitous, so security is no longer just something for "professionals" to consider
  - How do we protect our personal lives?

- Internet usage has significantly changed how the world does business
  - Supposedly "more at stake" than individuals, and a "richer target" for malicious actors – but how can organisations keep ahead of the current threats and vulnerabilities?

Managing Security = Managing Risk

A "completely secure" machine is an unusable machine

What is the right balance between security and usability?

What are the inherent risks that we accept?

Complete Security

Complete Convenience / Usability

Where on the spectrum do we wish to sit?

What is an appropriate Risk Appetite?

UWE Bristol University of the West of England

Case Studies

WannaCry

- May 12th -15th 2017
- Ransomware Cryptoworm
- 230,000 computers, 150 countries
- EternalBlue exploit of Server Message Block (SMB) to spread
- Microsoft patched supported systems in April 2017 – however Windows XP was not supported
- Spread was stopped "accidentally" by Marcus Hutchins – the kill switch was a URL that he registered
- In December 2017, US, UK, and Australia formally assert North Korea as being behind the attack

https://en.wikipedia.org/wiki/WannaCry_ransomware_attack

Equifax

- Discovered on July 29th 2017
- 145,000,000 consumers in the US
- Credit scoring agency
- Names, social security numbers, birth dates, addresses, driving license numbers, 209,000 credit card numbers.
- Vulnerability in a web application
- 44% of the US population will feel the impact of this breach
- Offering one year free credit monitoring and identity theft insurance – but what about in years to come?

UWE Bristol | University of the West of England

https://www.wired.com/story/how-to-protect-yourself-from-that-massive-equifax-breach/
https://www.bbc.co.uk/news/technology-43241939

Stuxnet

- Iran Nuclear Facility
- Malware infection of control systems
- Designed to speed up centrifuge rotation, and block monitoring controls
- Resulted in damage and explosion of facilities, and employees being fired
- Delay to Iran weapons programme
- Described as "Cyber Warfare"
- Suggested that attack was from US
- A "cyber" attack with physical consequence…

https://www.digitaltrends.com/computing/bits-before-bombs-how-stuxnet-crippled-irans-nuclear-dreams/

Beyond Cyber Security

- In 2005, Hurricane Katrina went down in history as the costliest and one of the deadliest natural disasters to strike the U.S., with damage to property costing $150 billion and nearly 2,000 people losing their lives.

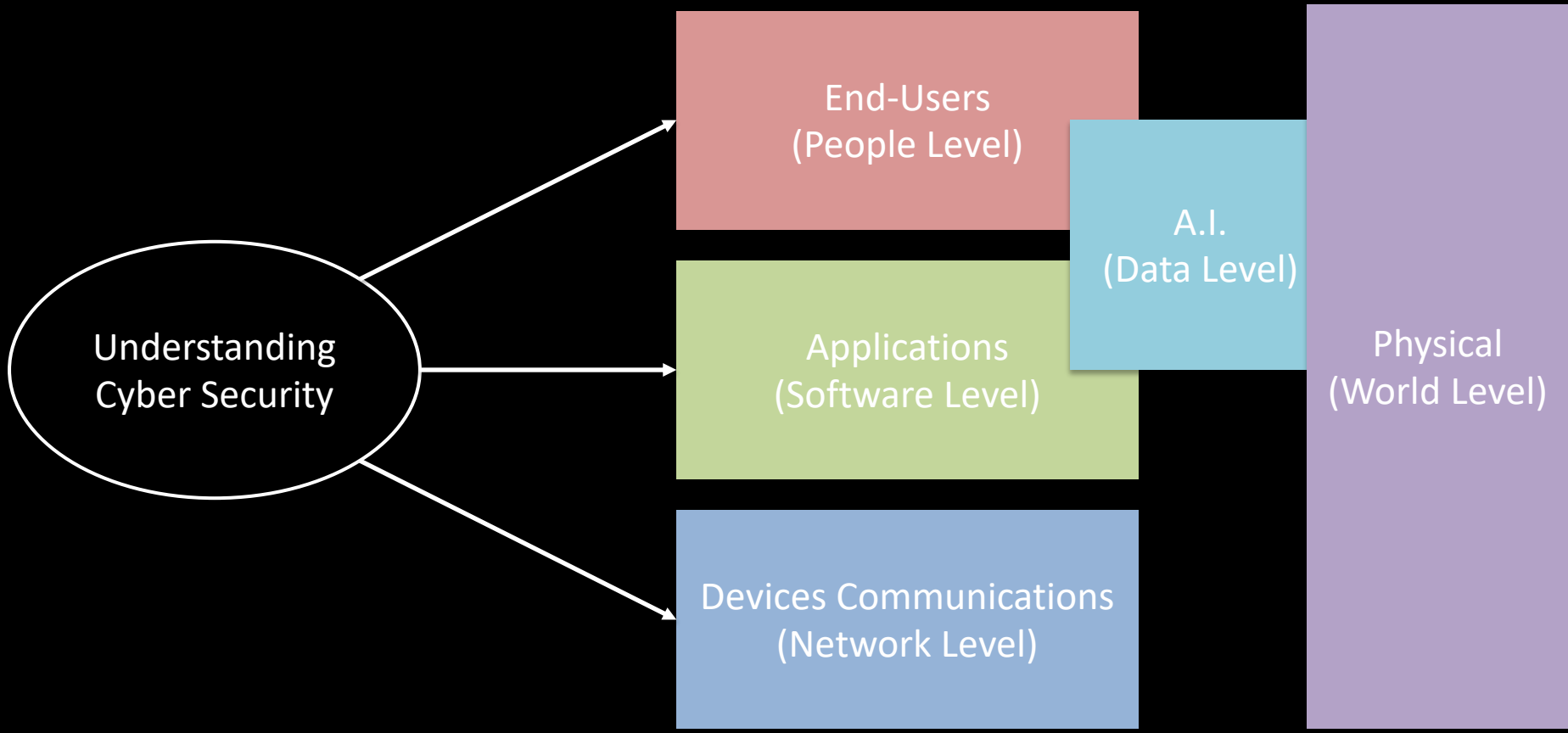
- On 14th June 2017, 72 people died in the fire at Grenfell Tower in London. The fire was started accidentally by a malfunctioning fridge-freezer on the fourth floor.

UWE Bristol | University of the West of England

Beyond Cyber Security

- What is cyber security without factoring in the physical security that surrounds us?

- Risk management?
- Understanding people?
- Multi-site data recovery / backup?
- Critical National Infrastructure?
  - Gas / power stations / water treatment?
- Disaster recovery?



Understanding Cyber Security

- Protection of what we hold most valuable – wellbeing, and personal data
- Protection of what our organisations hold most valuable – intellectual property, data records, infrastructure, assets
- Recognising the implications of technology in modern society – what are the risks we accept, what are the risks we need to reject, and what are the potential risks that we may overlook?
- A **skills-gap** due to rapid advancement in the area (estimated around 1.5 million people needed) – there is a great need to promote security awareness and understanding

"With great power comes great responsibility"

UWE Bristol | University of the West of England

MSc Cyber Security at UWE

- UWE is NCSC-certified for MSc Cyber Security

- We are offering 3 fully-funded postgraduate bursaries for the MSc Cyber Security, funded by the Department of Digital, Culture, Media and Sport (DCMS).
  - Announced TODAY by DCMS
  - UWE details will be following in the coming days.

- Bursaries are available to those who want to move into a career in Cyber Security from other areas. Emphasis of the DCMS also aims to encourage females to enter this industry.

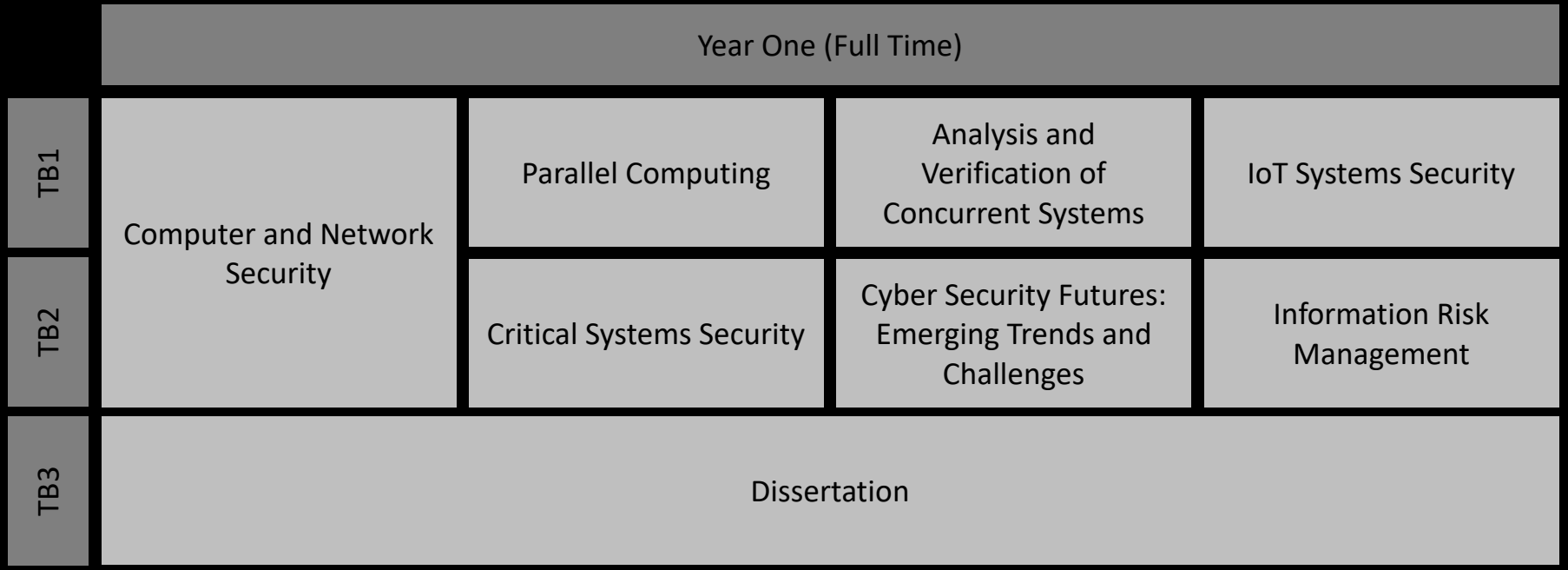
National Cyber Security Centre
a part of GCHQ

Department for Digital, Culture, Media & Sport

UWE Bristol | University of the West of England

https://www.ncsc.gov.uk/information/ncsc-certified-degrees

MSc Cyber Security at UWE



UWE Bristol | University of the West of England

Full Time Programme

MSc Cyber Security at UWE

	Year One (Part Time)		Year Two (Part Time)	
TB1	Computer and Network Security	Parallel Computing	Analysis and Verification of Concurrent Systems	IoT Systems Security
TB2		Information Risk Management	Cyber Security Futures: Emerging Trends and Challenges	Critical Systems Security
TB3			Dissertation	

UWE Bristol | University of the West of England

Part Time Programme

Thank you

Phil.Legg@uwe.ac.uk
@dr_plegg
http://go.uwe.ac.uk/phil
http://www.plegg.me.uk

UWE Bristol | University of the West of England