Systems Design and Security

Part 2: Information Security

http://staffwww.dcs.shef.ac.uk/people/A.Simons/

Home ⇒ Teaching ⇒ Lectures ⇒ COM2008/COM3008

The University Of Sheffield.

Bibliography

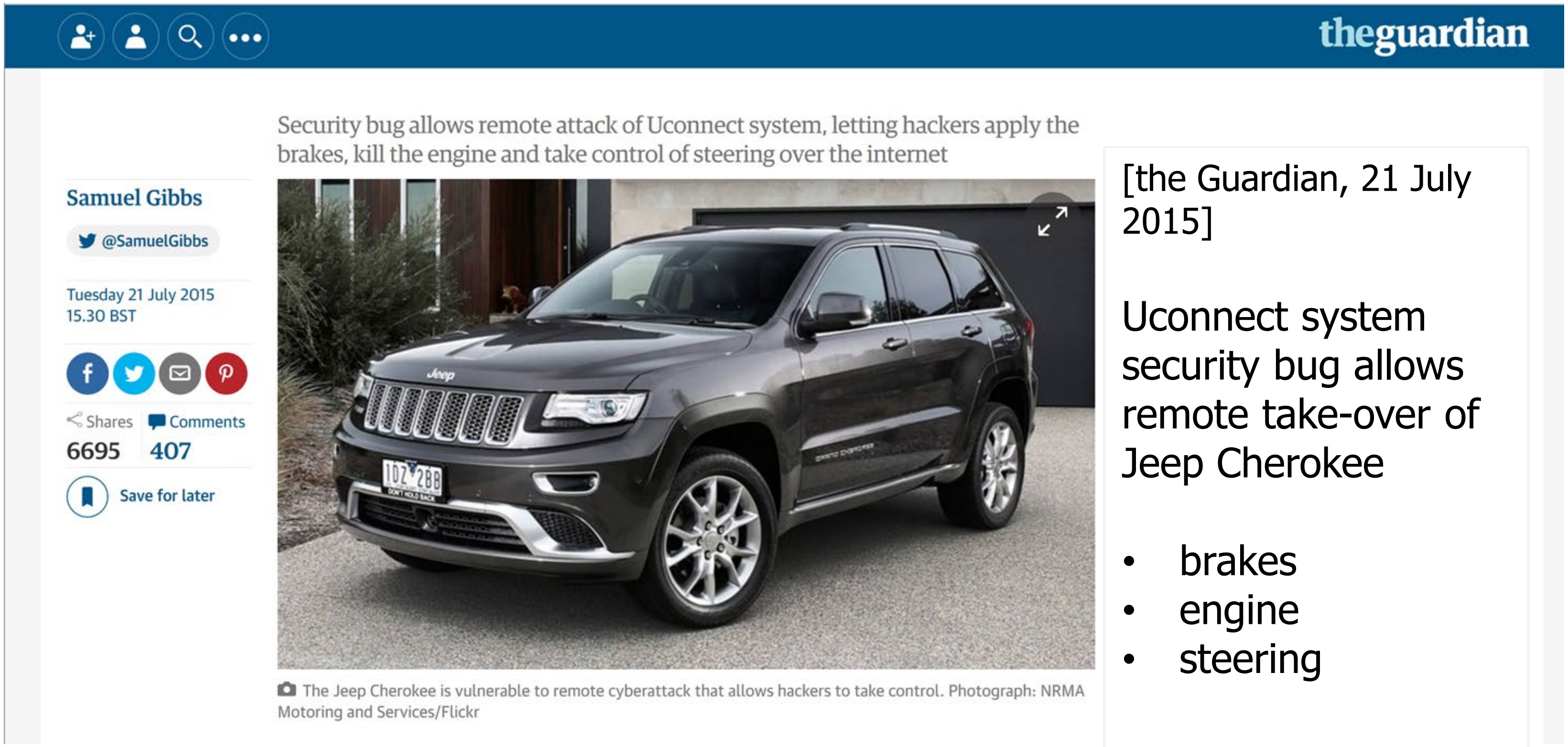
- Software Engineering
  - I Sommerville. Software Engineering, 10th ed., Pearson, 2016. Part 2: Dependability and Security, Chaps. 10-14.
  - R S Pressman, B R Maxim. Software Engineering: A Practitioner's Approach, 9th ed., McGraw-Hill, 2019. Part 3: Quality and Security, Chaps. 15-18.
- Security Engineering
  - R Anderson. Security Engineering, 2nd ed., John Wiley, 2008.
    - Also online: https://www.cl.cam.ac.uk/~rja14/book.html
  - M Goodrich, R Tamassia. Introduction to Computer Security, Pearson, 2010.

Outline

- Security threats
  - How they're out to get you
- Vulnerabilities
  - Technical and social attacks
- Countermeasures
  - Technical and social defences
- Security policies
  - Succinct statement of protection strategies
- Legal obligations
  - Data Protection, Computer Misuse, GDPR

Reading: Sommerville ch. 13-14; Anderson ch. 1-3

Cyber Carjack!



theguardian

Security bug allows remote attack of Uconnect system, letting hackers apply the brakes, kill the engine and take control of steering over the internet

Samuel Gibbs

@SamuelGibbs

Tuesday 21 July 2015
15.30 BST

Shares 6695

Comments 407

Save for later

The Jeep Cherokee is vulnerable to remote cyberattack that allows hackers to take control. Photograph: NRMA Motoring and Services/Flickr

[the Guardian, 21 July 2015]

Uconnect system security bug allows remote take-over of Jeep Cherokee

- brakes
- engine
- steering

Cybersecurity

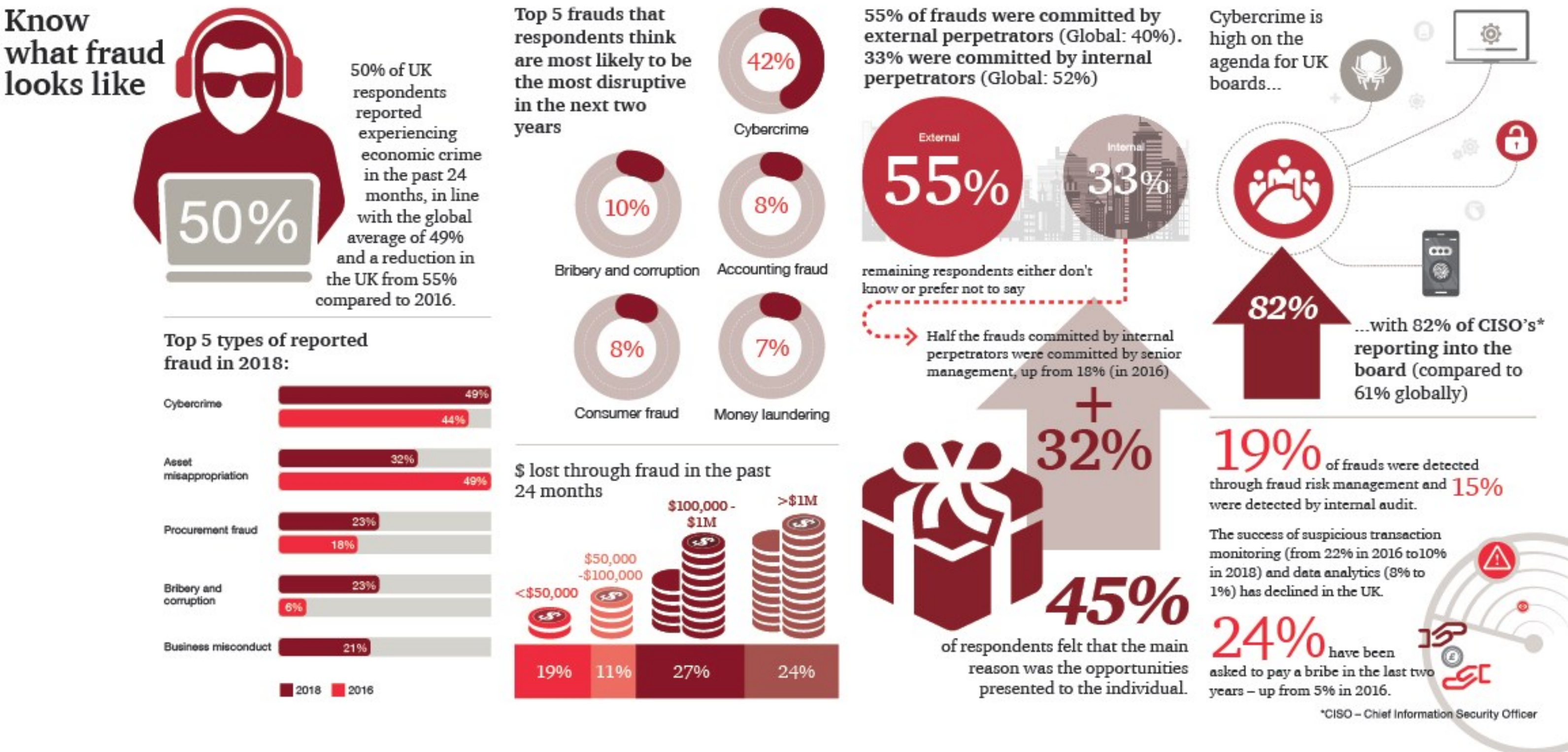
- Hot topic
  - huge cyber threat increase in last decade
  - not just white hat, black hat hackers
  - organised criminals, nation states
  - cyber attack ranked #3 threat to UK
    - after terrorism, espionage, cybercrime, WMD proliferation
- Domains

[https://www.cpni.gov.uk/national-security-threats]

  - financial (credit cards, bank details)
  - information (state secrets, exam papers)
  - software (downloaded, uploaded programs)
  - hardware (aircraft, nuclear power stations)
  - democracy (troll armies, social media harvesting)

The University Of Sheffield.

UK/Global Fraud



Know what fraud looks like

50% of UK respondents reported experiencing economic crime in the past 24 months, in line with the global average of 49% and a reduction in the UK from 55% compared to 2016.

Top 5 types of reported fraud in 2018:

Top 5 frauds that respondents think are most likely to be the most disruptive in the next two years

$ lost through fraud in the past 24 months

55% of frauds were committed by external perpetrators (Global: 40%). 33% were committed by internal perpetrators (Global: 52%)

remaining respondents either don't know or prefer not to say

Half the frauds committed by internal perpetrators were committed by senior management, up from 18% (in 2016)

45% of respondents felt that the main reason was the opportunities presented to the individual.

Cybercrime is high on the agenda for UK boards...

...with 82% of CISO's* reporting into the board (compared to 61% globally)

19% of frauds were detected through fraud risk management and 15% were detected by internal audit.

The success of suspicious transaction monitoring (from 22% in 2016 to10% in 2018) and data analytics (8% to 1%) has declined in the UK.

24% have been asked to pay a bribe in the last two years – up from 5% in 2016.

*CISO – Chief Information Security Officer

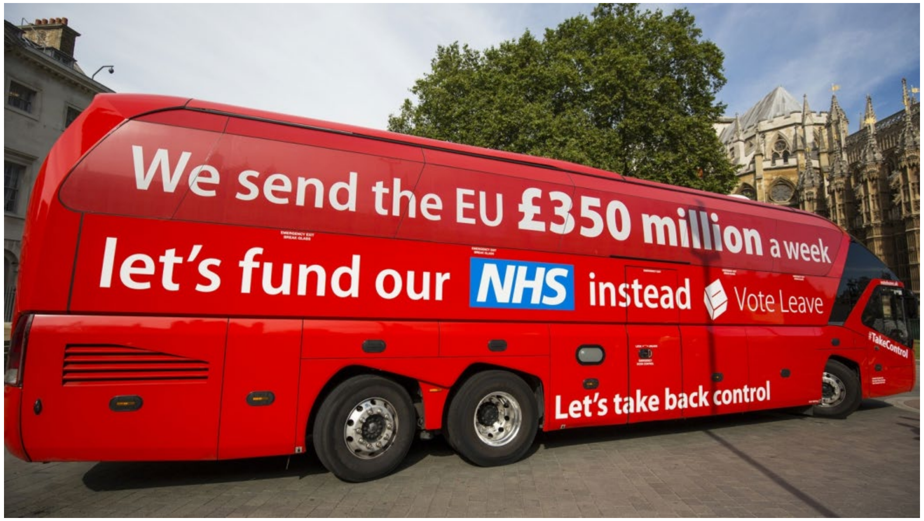
[https://www.pwc.co.uk/services/forensic-services/insights/global-economic-crime-survey-2018---uk-findings.html]

Cyber Attack Types

- Deliberately cause havoc, for fun
  - early so-called "white hat" hackers
- Obstruct, block, deny your services
  - online bots posting millions of requests
- Snoop on, steal from, impersonate you
  - phishing, social engineering, pretexting
- Modify, delete, damage your data
  - viruses, trojans, ransomware
- Manipulate public opinion, fake news
  - robot Twitter accounts, troll-farms
- Subvert elections, referenda, democracy

Fake News: Facebook

[https://www.independent.co.uk/voices/michael-gove-boris-johnson-brexit-eurosceptic-press-theresa-may-a7533806.html]


We send the EU £350 million a week
let's fund our NHS instead
Vote Leave
Let's take back control
#TakeControl

[https://www.irishtimes.com/opinion/cliff-taylor-no-end-in-sight-for-fake-news-and-post-truth-1.3336523]

Fact check: Brexit result cost 15 years' of EU membership *overnight* in lost value
Since then, roughly £300m per week, or £20bn to 2022, or -1.3% GDP

[https://www.independent.co.uk/news/business/news/brexit-uk-economy-losses-eu-referendum-result-billions-leave-european-union-a8081841.html]

Truth Crisis?

Complete denial of climate change

Political agenda based on fake news
- trade tariffs
- Mexican wall
- drain the swamp

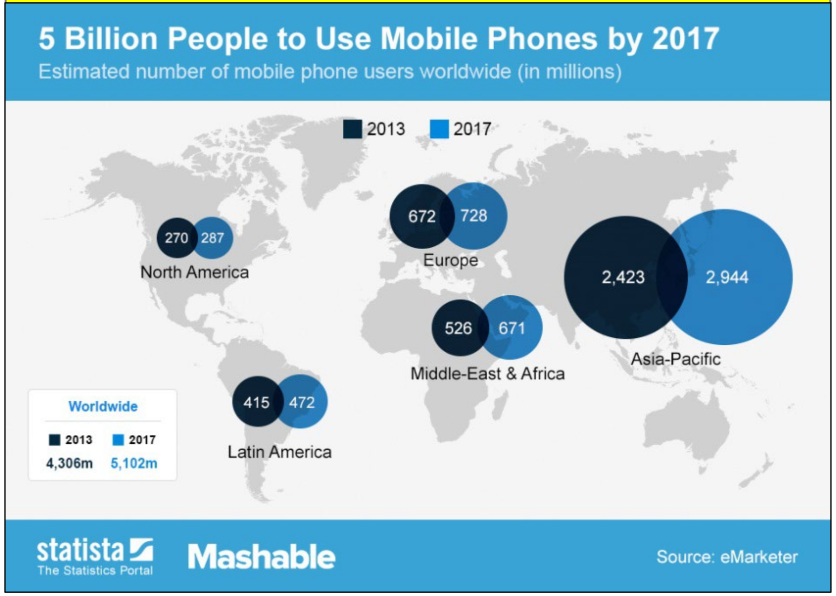
Russian troll-farm involvement in US elections?

[https://eu.usatoday.com/story/news/2022/09/06/analysis-trump-faces-gathering-storm-presidency-possible-consitutional-crises/1210194002/]

Information

- Information is ubiquitous
  - a valuable organisational asset
  - need access to information to do our jobs
  - many forms: in conversation, on paper, online
- Increasing amounts of online information
  - interaction with companies and public services
  - freely offering personal information, especially younger generation

"Information is the oxygen of the modern age." (Ronald Reagan, 1989)



[https://www.statista.com/chart/1517/worldwide-mobile-phone-users/]

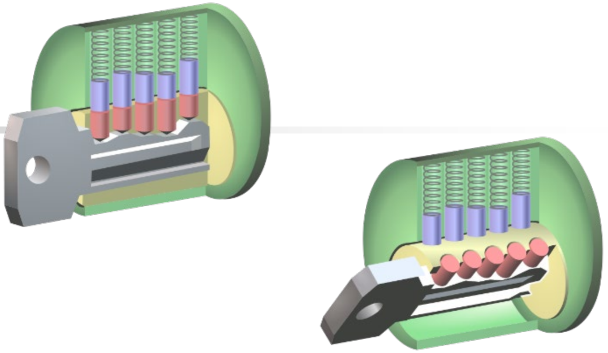
Online Benefits

- E-commerce leads to more efficient and more convenient ways of doing business
- Smart cities/smart grids leads to enhanced energy efficiency
- Connected healthcare enhances patient experience and outcomes by faster access to relevant medical data
- Online banking and shopping frees up time for other priorities
- Online learning makes education more accessible to many
- Social networking enables more people to be connected to friends, family, job opportunities and more

[https://cphcuk.files.wordpress.com/2014/11/perspectives_integrating-cybersecurity-into-computer-science-curricula-final31102014.pdf]

How Safe?

- Physical security
  - Building, office, cabinet
  - Locks, cards and magnetic strips, passcodes, …
- Information security
  - Protection of assets
  - Policies, encryption, access control
- Network and communication security
  - Authentication, protocols, encryption
  - Firewalls, anti-virus software, VPN, https…

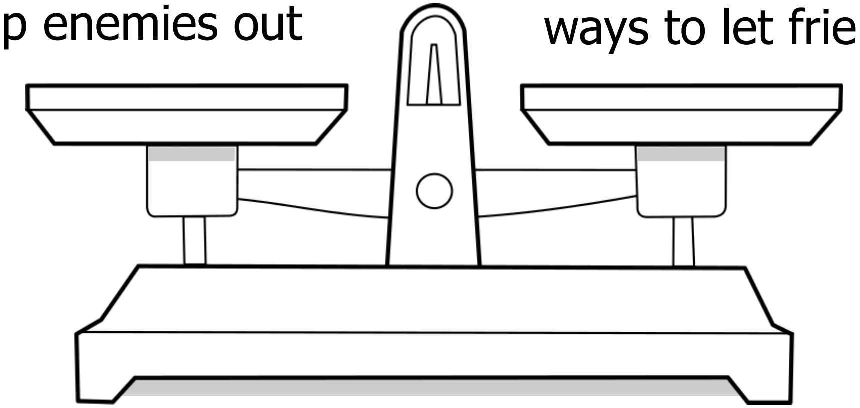


[http://www.sheffield.ac.uk/cics/ucards]

["Pin tumbler with key" by Derivative work: Pbroks13; Original: Wapcaplet - File:Pin tumbler with key.png. Licensed under CC BY-SA 3.0 via Commons - https://commons.wikimedia.org/wiki/File:Pin_tumbler_with_key.svg#/media/File:Pin_tumbler_with_key.svg; and File:Pin_tumbler_unlocked.svg]

Balance of Protection

- Want to protect against malicious attacks
  - whether from outsiders or insiders
- Want to keep open for fair and proper use
  - maximum security, minimum impact on productivity



Lab 1: Quick Login

Run a Poll

- Imagine you are building...
  - a software system for a student project
  - it has password-protected access for users
  - as the developer, you want to test new features regularly
  - you want to get in and out of the system quickly
- What login ID and password?
  - write down a typical username and password you would use for this, as your admin login
  - write down another username and password, if you have more than one typical admin login
  - be honest about what you would choose, given that the system is a fairly low-risk one

Security Terminology

- Assets
  - what you wish to protect
  - how valuable they are
- Vulnerabilities
  - weaknesses that make attack possible
  - could be technical, or social/behavioural
- Threats
  - potential dangers to your assets, estimated loss
  - threats take advantage of vulnerabilities
- Attacks
  - actions leading to violation of security
- Countermeasures
  - what you can do to prevent/minimise attacks

Assets

£450K - £5M

£17K - £44K

- What do you want to protect?
  - how much effort to protect each of these ?

["Aston.db5.coupe.300pix". Licensed under Public Domain via Commons - https://commons.wikimedia.org/wiki/File:Aston.db5.coupe.300pix.jpg#/media/File:Aston.db5.coupe.300pix.jpg]

["Trotters" The original uploader was Goldfinger at Serbian Wikipedia - Transferred from sr.wikipedia to Commons by BokicaK using CommonsHelper.. Licensed under CC BY 3.0 rs via Commons - https://commons.wikimedia.org/wiki/File:Trotters.jpg#/media/File:Trotters.jpg]

- Quantify the risk to each asset
  - likelihood of being targeted by attack
  - probability of attack being successful
  - estimated impact of successful attack

Vulnerabilities - I

- Backdoors
  - secret routes into software left by developers
  - later exploited by hackers, or developers!
- Direct access
  - left or lost disks, flash drives
  - unsecured networks, laptops
- Eavesdropping
  - sniffing traffic going through routers
  - inferring data from EM waves, energy usage
- Spoofing
  - keyloggers used to detect password entry
  - steal and use another person's identity

Open Door?

I changed my password to "incorrect". So, whenever I forget what it is, the computer will say "Your password is incorrect".

Rank	2020	2021	Chart
1	123456	123456	no change
2	123456789	123456789	no change
3	picture1	12345	up 5
4	password	qwerty	new entry
5	12345678	password	down 1
6	111111	12345678	down 1
7	123123	111111	down 1
8	12345	123123	down 1
9	1234567890	1234567890	no change
10	senha	1234567	new entry

Survey of the most common passwords (as revealed in data breaches)

[http://nordpass.com]

[http://logos.wikia.com/wiki/Top_of_the_Pops]

Data Breaches

- Jan 2009: health worker lost memory stick with medical records of 6000 prisoners; encrypted, but with password on a sticky-note
- Oct 2008: hard-drive lost with MOD data on 100,000 armed forces personnel, inc. bank details, passport, DoB, driving license, telephone numbers
- Jun 2008: Cabinet Office intelligence officer left file marked "UK Top Secret" on train with Al-Qaeda and Iraq vulnerability details
- Nov 2007: HMRC lost two disks with 25m child benefit records in the internal post, with name, address bank details, NI numbers of 2.75m families

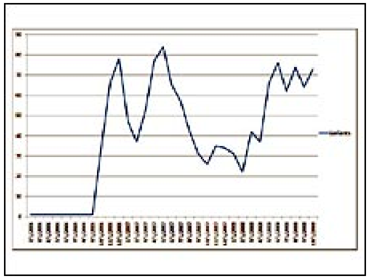
BBC [http://news.bbc.co.uk/1/hi/uk/7449927.stm]

[http://www.cambridgeed.com/PLAN-Test/Assessments-and-Data/pl04-1-1568/
https://www.amazon.ca/White-Train-Model-Flash-Memory/dp/B079DJKXH4]

Vulnerabilities - II

- Trojans, viruses, worms
  - malware hiding inside regular software
  - worm viruses attached to end of data blocks
  - used for data tampering, keylogging
- Privilege escalation
  - enter system using end-user privileges
  - get higher authorisation, up to root access
- Denial-of-service
  - overload machine, bandwidth, trigger a lockout
  - DDOS (distributed denial of service) using a botnet
- Clickjacking
  - redirect web access, fake login pages, password sniffing

Trojan



- Feb 2006: security firm RSA found that 270K online bank accounts and 240K credit, debit card details stolen by Windows Sinowal trojan
- RSA found Sinowal works as a drive-by download: just visiting an infected website can load it
- Sinowal also known as Torpig or Mebroot, operated secretly for 2 years before detection

- Apr 2007: Google found 1 in 10 of 4.5m surveyed web pages to be infected
- May 2008: Sophos found rate of infection was 6K pages per day
- Sept 2008: Fortinet reported attacks rising from 10m to 30m. Source appears to be Russia, or E. Europe

BBC [http://news.bbc.co.uk/1/hi/technology/7701227.stm]

Top 8 Viruses

All-time most destructive, collated by Norton in 2016

- CryptoLocker: 2013 ransomware spread by email attachment; encrypted all your files; pay to decrypt. Cost $30m in 100 days
- ILOVEYOU: 2000 worm that overwrote files. Cost $15bn
- MyDoom: 2004 hit Google, SCO, Microsoft with DDOS; also sent spam email. Cost $38bn
- StormWorm: 2006 fake news link installed a botnet that spread spam. Cost unknown

[https://uk.norton.com/norton-blog/2016/02/the_8_most_famousco.html]

- Sasser/Netsky: 2004 created by German teen to outdo MyDoom. Shut down transatlantic flights. Cost $31bn
- Anna Kournikova: 2001 click-bait worm that copied itself to address books. Harmless, but cost $166K to fix
- Slammer: 2003 fast-spreading UDP worm that crashed half the Internet. Cost $1bn.
- Stuxnet: 2010 first ever digital weapon deployed by US against Iran nuclear facilities. Caused centrifuges to self-destruct

Social Engineering

- Phishing
  - attacker impersonates a trustworthy source
  - tries to get you to divulge personal info
  - often uses URL link-shorteners to conceal redirection
  - often uses phone/email password scams
- Pretexting
  - plausible fabricated role-play scenario to elicit information
  - phone call offering to help fix a (non-existent?) problem
  - attacker asks victim to confirm identity
- Baiting
  - infected disks, web pages with attractive content (click-bait)
  - promise of free stuff if you give your credentials (quid pro quo)
  - leave infected flash drives around to see if you plug one in

Media Manipulation

- Sockpuppets
  - robot accounts created on Twitter or Facebook
  - adjust balance of opinions, act as voice-multiplier
- Troll armies
  - organised teams of Twitter, Facebook posters
  - used to promote one side in a campaign, election or referendum
  - form of state attack used by Russia, USA
- Astroturfing
  - above tricks used to create fake groundswell of popular opinion (fake "grass-roots")
  - sometimes start by deliberately posting contrary arguments, to trigger a bigger desired counter-response

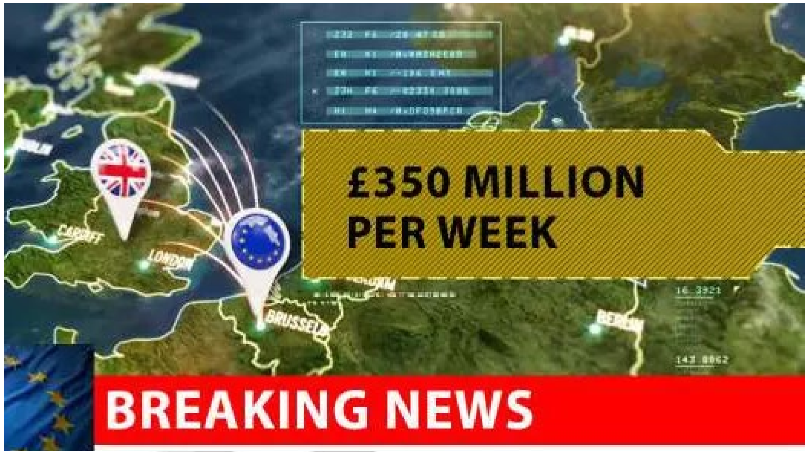
Prediction come True!

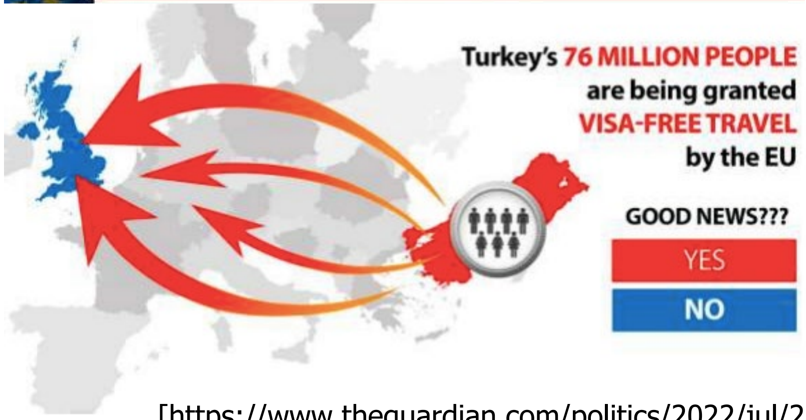
Howard Gordon and Alex Gansa.
© Showtime, Fox 21 Television

Clip from Homeland, Season 6, 2016.
[https://www.youtube.com/watch?v=EufH0T196bY]

UK Commons Select Committee on Digital, Culture, Media & Sport

Cambridge Analytica, 2018





Turkey's 76 MILLION PEOPLE are being granted VISA-FREE TRAVEL by the EU
GOOD NEWS???
YES
NO

- CA boss Alexander Nix, Facebook's Mark Zuckerberg testify to DCMS Committee
- Facebook forced to reveal "dark adverts" targeted at vulnerable users
- Users were harvested by CA from insecure research app
- Fake ads commissioned by Vote Leave campaign from Canadian agency AggregateIQ

Lie: Turkey is not about to join EU

[https://www.theguardian.com/politics/2022/jul/28/dcms-committee-report-finds-truth-fake-news-facebook-brexit]

Countermeasures -I

- Authentication and authorisation
  - secure user accounts with password protection
  - access-controls, privileged users may access specific data
- Multi-factor authentication
  - requires 3+ items: user ID, password, memorable info
  - sometimes requires physical key, a "dongle"
- Firewalls
  - shield internal network services from attacks
  - perform packet-filtering on external traffic
- Secure networking
  - HTTPS: client/server authentication using private/public key
  - encrypted data transfer, e.g. for login portals
  - Virtual Private Networks (VPNs) tunnelling through

Countermeasures -II

- Physical separation
  - physically separate networks, computers (no Internet)
  - secure room inside a Faraday cage (blocks EM)
- Cryptography
  - message digests (proof of no tampering in transit)
  - digital certificates (proof of origin of software, message)
  - non-repudiation (proof of bilateral transaction)
  - confidentiality (encryption provides secrecy)
- Intrusion detection
  - packet-logging systems for forensics
- Formal verification
  - secure O/S or hypervisor (secure installer, service layer)
  - blocks malware, installs only trusted modules

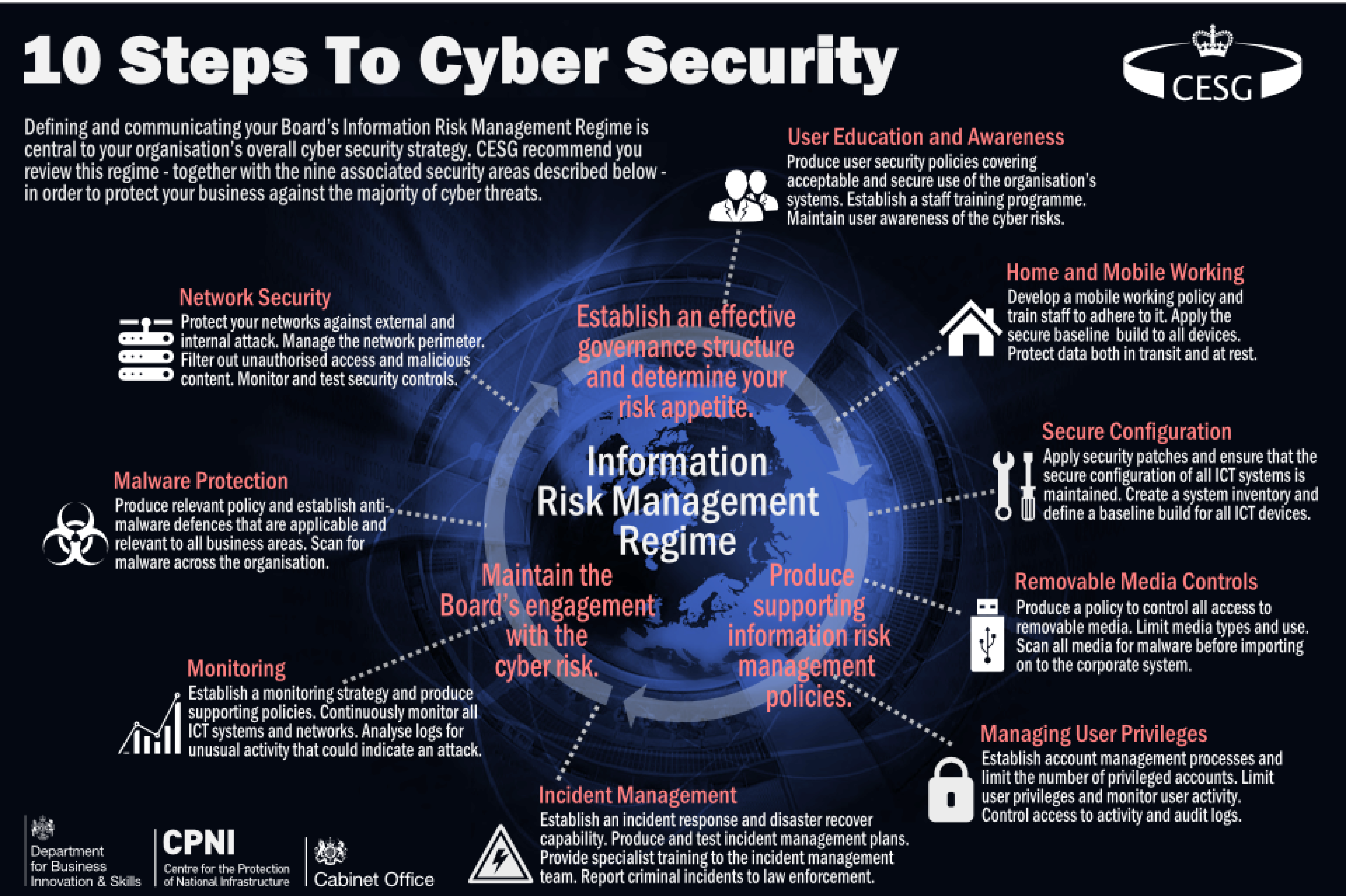
Cyber Security Training

- Social countermeasures
  - training in correct use of machines, networks, passwords
  - training in anti-phishing, pretexting, baiting scams
  - avoid tailgating into secure areas, impersonation
- Subversion countermeasures
  - education about Facebook, Twitter post-truth "reality"
  - use fact-check sites: e.g. Channel 4 News
  - legislation against disinformation - Germany, 2017 new bill fines providers €50m for breaking rules
  - Facebook suspended 30K fake news sites in France
  - Twitter regularly shuts down abusive bots
  - problems balancing this with freedom of speech - UK typically vague about what it will do

Threats to UK

- CPNI: Centre for Protection of National Infrastructure
  - responsible for protecting UK national infrastructure
  - responsible directly to MI5
  - see: https://www.cpni.gov.uk/
- Ranked top threats in 2022
  - terrorism: targeting UK businesses, economy, transport infrastructure
  - espionage: covertly obtaining military, industrial, political secrets, compromise security
  - cybercrime: by foreign states, criminals, terrorists and hacktivists, espionage and network attack
  - proliferation: of nuclear, biological, chemical weapons of mass destruction, sourced from weak states

https://www.gov.uk/government/publications/cyber-risk-management-a-board-level-responsibility/10-steps-summary



10 Steps To Cyber Security

CESG

Defining and communicating your Board's Information Risk Management Regime is central to your organisation's overall cyber security strategy. CESG recommend you review this regime - together with the nine associated security areas described below - in order to protect your business against the majority of cyber threats.

Information Risk Management Regime

Establish an effective governance structure and determine your risk appetite.

Produce supporting information risk management policies.

Maintain the Board's engagement with the cyber risk.

User Education and Awareness

Produce user security policies covering acceptable and secure use of the organisation's systems. Establish a staff training programme. Maintain user awareness of the cyber risks.

Home and Mobile Working

Develop a mobile working policy and train staff to adhere to it. Apply the secure baseline build to all devices. Protect data both in transit and at rest.

Secure Configuration

Apply security patches and ensure that the secure configuration of all ICT systems is maintained. Create a system inventory and define a baseline build for all ICT devices.

Removable Media Controls

Produce a policy to control all access to removable media. Limit media types and use. Scan all media for malware before importing on to the corporate system.

Managing User Privileges

Establish account management processes and limit the number of privileged accounts. Limit user privileges and monitor user activity. Control access to activity and audit logs.

Incident Management

Establish an incident response and disaster recover capability. Produce and test incident management plans. Provide specialist training to the incident management team. Report criminal incidents to law enforcement.

Monitoring

Establish a monitoring strategy and produce supporting policies. Continuously monitor all ICT systems and networks. Analyse logs for unusual activity that could indicate an attack.

Malware Protection

Produce relevant policy and establish anti-malware defences that are applicable and relevant to all business areas. Scan for malware across the organisation.

Network Security

Protect your networks against external and internal attack. Manage the network perimeter. Filter out unauthorised access and malicious content. Monitor and test security controls.

Department for Business Innovation & Skills

CPNI Centre for the Protection of National Infrastructure

Cabinet Office

Multi-layered Policies

- Physical Security
  - physical barriers, locked resources, access control
  - monitoring, intruder/threat detection
  - command & control, defence in depth
- Personnel & People Security
  - policies that mitigate against insider attacks
  - vetting personnel, promoting security culture
  - disrupting hostile reconnaissance
- Cyber Security
  - network and information systems hardening
  - e.g. Protective DNS for public sector - extra firewalling
  - National Cyber Security Centre, launched 2017

Lab 2: Security Policy

- What is your security policy?
  - make a list of your assets
  - identify vulnerabilities
  - identify threats, attacks
  - identify countermeasures
- How would you deal with:
  - a fire in your residence
  - the theft of your laptop
  - hard-disk crash on your laptop
  - a virus transmitted by email
  - a vulnerability found in your O/S
  - sharing a friend's memory stick
  - tailgating you through the Diamond/Info. Commons

Run a Poll

Legal Obligations

- Computer Misuse Act, 1990
  - prohibits hacking for malicious purposes
- Human Rights Act, 1998
  - enshrines freedoms, especially to privacy
- Data Protection Act, 1998
  - sets limits on the holding of personal data
- Investigatory Powers Act, 2016
  - allows traffic monitoring for security reasons
- General Data Protection Regulation, 2018
  - strengthens all the above across the EU

Computer Misuse Act, 1990

- Computer misuse offences
  1) Unauthorised access to computer material
  2) Unauthorised access with intent to commit or facilitate commission of further offences
  3) Unauthorised acts with intent to impair, or with such recklessness as to impair, operation of computer, etc.
  4) Unauthorised acts causing, or creating risk of, serious damage
  5) Making, supplying or obtaining articles for use in offence under 1, 3 or 4

[http://www.legislation.gov.uk/ukpga/1990/18/contents]

Data Protection Act, 1998

- Controls how your personal information is used by organisations, businesses or the government
- Must make sure the information is:
  - used fairly and lawfully
  - used for limited, specifically stated purposes
  - used in a way that is adequate, relevant and not excessive
  - accurate
  - kept for no longer than is absolutely necessary
  - handled according to people’s data protection rights
  - kept safe and secure
  - not transferred outside the European Economic Area without adequate protection
- Information Commissioner's Office
  - https://ico.org.uk/ - authority promoting public openness and data privacy for individuals, with controlled information access rights

Investigatory Powers Act, 2016

- So-called snooper's charter, allowing UK intelligence and police agencies to carry out
  - targeted interceptions of communications
  - bulk collection of communications data
  - bulk interception of communications
  - targeted hacking of devices for national security reasons
- Requires Communication Service Providers to
  - record all websites visited for 1 year (but not the individual pages)
  - allow police access to such records without warrant
- Investigatory Powers Commission
  - panel of judges, who regulate application of law
  - intended as a check and balance

EU General Data Protection Regulation, 2018

- Individual rights
  - data protection by design and by default
  - privacy for all personal data, records, images
  - right to give, withdraw consent for data use
  - right of access to data, how long it is kept for use
- Corporate responsibilities
  - anonymisation/pseudonymisation of personal data
  - data held securely, encrypted, privacy protected
  - data held only for legitimate contractual purposes
  - data retained only as long as needed (no sharing)
- Regulatory framework
  - Data Controller appointed in each business
  - Data Protection Authority set up in EU member states

Identity Theft

Clip from CIFAS - UK Fraud Prevention Service

[https://www.cifas.org.uk/services/identity-protection]

Security and You

- Do you [vulnerability] [threat] [risk]
  - regularly update your anti-virus software?
    - [no update] [virus attack] [destruction of ...]
  - make back-ups of your files?
    - [no backup] [theft/disk-crash] [loss of project ...]
  - forward warning emails to your friends?
    - [no action] [not forewarned] [spread of virus]
  - use a secure password with 8+ chars, symbols and digits?
    - [short password] [easy to crack] [impersonation, data loss]
  - regularly apply security patches to your laptop?
    - [disregard patches] [open to attack] [computer crash/corruption]

Summary

- Cyber security is a hot topic, now judged to be the no. 3 threat to the UK
- Historic cyber attacks were benign intrusions by hackers, malicious viruses exploiting O/S weaknesses
- Organised cyber attacks by criminals, nation states are a larger economic threat: fraud, espionage, terrorism
- Recent cyber attacks harvesting social media to target individuals have manipulated elections, referenda
- Defence in depth only comes through a layered security policy: physical, personal, technical; and education
- Personal cyber security means that you need to be aware of threats, take defensive measures while a student