THALES

Human Factors in London's Cyber Defence

Amanda Widdowson, Human Factors Capability Lead

Why is Human Factors relevant to cyber security?

"60% of all attackers are insiders" (IBM 2016)

"Over 95% of ..breaches are caused by human error" (IBM 2015)

- How do we address the human element in cyber security?

- Approach to measure & mitigate the risk of *human*-related cyber security vulnerabilities

THALES

What is at risk? Transport

Urban rail

- Driverless trains - increased use of autonomous agents (e.g. Siri, Alexa)
- Signalling systems

River services

- Thames barrier

Road vehicles

- Driverless cars (future)
- Smartphone interface – synched to infotainment system

THALES

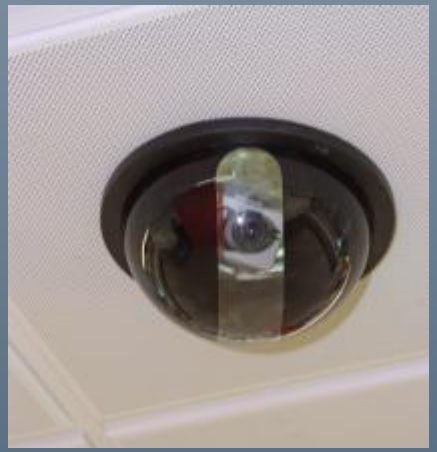
What is at risk?

- Smart city (& Smart homes)
- Building security (physical access to IT control systems)
- Utilities (electricity, gas, water)
- CCTV

THALES

Washington DC CCTV attack Jan 2017

- 70% of cameras stopped working (12th-15th Jan – before Trump inauguration)
- CCTV data storage devices were hacked (ransomware)



Human element

- Ransomware may have been result of clicking link or opening email attachment

THALES

Ukraine power grid attack Dec 2015

- Attack on electricity control centre shutdown substations affecting Kiev
- 250,000 customers lost power

Human element

- Email malware to electricity control centre employees
- Accessed login credentials

THALES

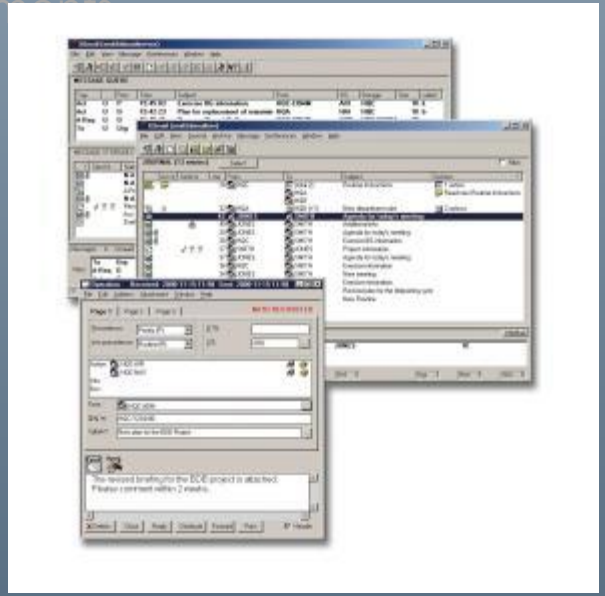
So how do we address the human element in cyber-security?

- Email management
- Investment of resources for cyber security
- Senior manager endorsement and behaviours (lead by example)
- Design policy around employees' work requirements
- Passwords
- Training
- Incident recording, reporting and analysis
- Recruitment, selection & monitoring
- Social media
- Tailgating
- Visitor management
- Remote/mobile working

THALES

So how do we address the human element in cyber-security?

- **Email management**
- Investment of resources for cyber security
- Senior manager endorsement and behaviours (lead by example)
- Design policy around employees' work requirements
- Passwords
- Training
- Incident recording, reporting and analysis
- Recruitment, selection & monitoring
- Social media
- Tailgating
- Visitor management
- Remote/mobile working



THALES

So how do we address the human element in cyber-security?

- Email management
- **Investment of resources for cyber security**
- **Senior manager endorsement and behaviours (lead by example)**
- Design policy around employees' work requirements
- Passwords
- Training
- Incident recording, reporting and analysis
- Recruitment, selection & monitoring
- Social media
- Tailgating
- Visitor management
- Remote/mobile working

THALES

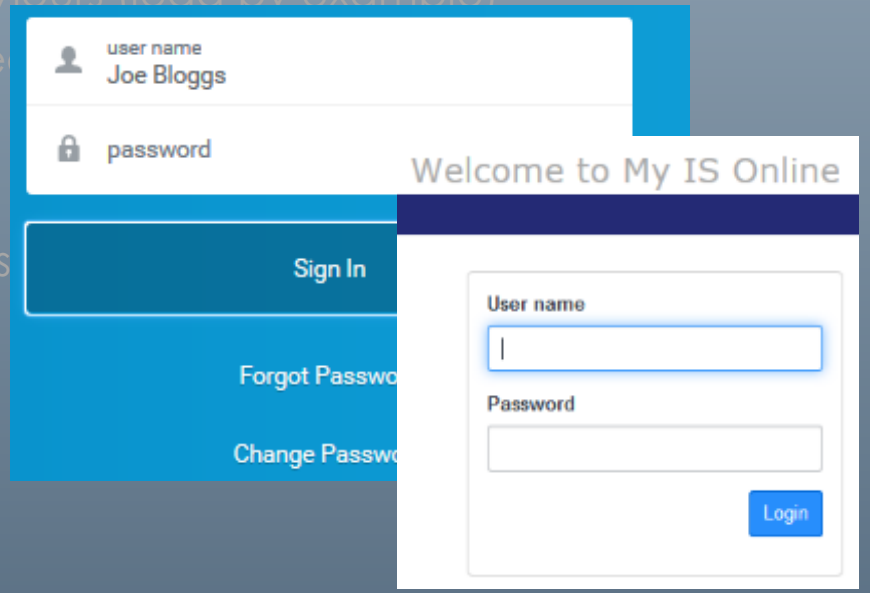
So how do we address the human element in cyber-security?

- Email management
- Investment of resources for cyber security
- Senior manager endorsement and behaviours (lead by example)
- **Design policy around employees' work requirements**
- Passwords
- Training
- Incident recording, reporting and analysis
- Recruitment, selection & monitoring
- Social media
- Tailgating
- Visitor management
- Remote/mobile working

THALES

So how do we address the human element in cyber-security?

- Email management
- Investment of resources for cyber security
- Senior manager endorsement and behaviours (lead by example)
- Design policy around employees' work re
- **Passwords**
- Training
- Incident recording, reporting and analysis
- Recruitment, selection & monitoring
- Social media
- Tailgating
- Visitor management
- Remote/mobile working



THALES

So how do we address the human element in cyber-security?

- Email management
- Investment of resources for cyber security
- Senior manager endorsement and behaviours (lead by example)
- Design policy around employees' work requirements
- Passwords
- **Training (real-world examples) & competence management**
- Incident recording, reporting and analysis
- Recruitment, selection & monitoring
- Social media
- Tailgating
- Visitor management
- Remote/mobile working

THALES

So how do we address the human element in cyber-security?

- Email management
- Investment of resources for cyber security
- Senior manager endorsement and behaviours (lead by example)
- Design policy around employees' work requ
- Passwords
- Training
- **Incident recording, reporting and analysis**
- Recruitment, selection & monitoring
- Social media
- Tailgating
- Visitor management
- Remote/mobile working

THALES

So how do we address the human element in cyber-security?

- Email management
- Investment of resources for cyber security
- Senior manager endorsement and behaviours (lead by example)
- Design policy around employees' work requirements
- Passwords
- Training
- Incident recording, reporting and analysis
- **Recruitment, selection & monitoring**
- Social media
- Tailgating
- Visitor management
- Remote/mobile working

THALES

So how do we address the human element in cyber-security?

- Email management
- Investment of resources for cyber security
- Senior manager endorsement and behaviours (lead by example)
- Design policy around employees' work requirements
- Passwords
- Training
- Incident recording, reporting and analysis
- Recruitment, selection & monitoring
- **Social media**
- Tailgating
- Visitor management
- Remote/mobile working

THALES

So how do we address the human element in cyber-security?

- Email management
- Investment of resources for cyber security
- Senior manager endorsement and behaviours (lead by example)
- Design policy around employees' work requirements
- Passwords
- Training
- Incident recording, reporting and analysis
- Recruitment, selection & monitoring
- Social media
- **Tailgating**
- **Visitor management**
- **Remote/mobile working**

THALES

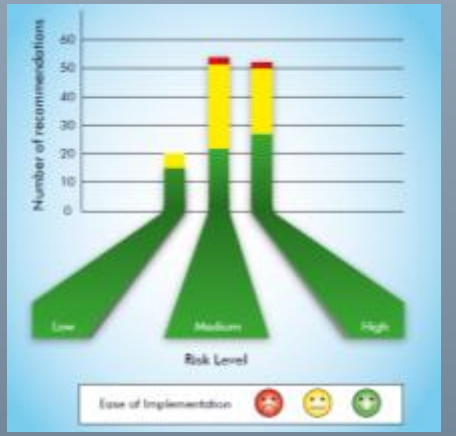
So how do we address the human element in cyber-security?

Cyber Human Error Assessment Tool (CHEAT)

- Human error assessment established in safety incidents
- Applied to cyber-security incidents

41 human error threat indicators with associated recommendations

4 categories



Purpose: to assess and mitigate human factors as part of

- Cyber Vulnerability Investigations (CVI)
- Cyber security (post) incident investigations

THALES

Conclusions

- **Consider the *human element* in order to reduce the risk of cyber security incidents**
- **Hard to change people, but there *are* actions we can take to reduce the risk of human-related cyber security incidents on our infrastructure**
- **Contact details:**

  - E: amanda.widdowson@uk.thalesgroup.com
  - M: +44 (0) 7583 419027

THALES