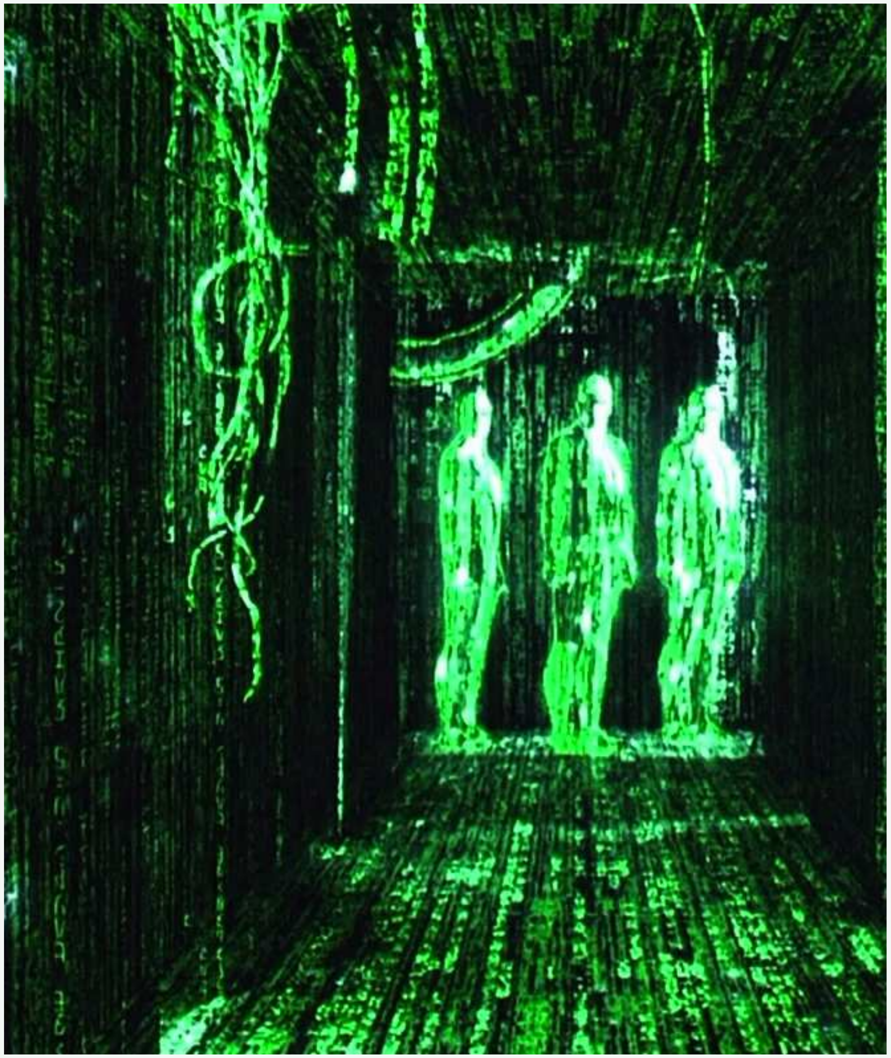
WOMEN'S CYBER FORUM 2017

The Cyber Environment

Launching Careers In Cyber Space

Content

- About myself
- Impact of digital technologies
  - On Society
  - On Security
- Organisation of Cyber Security
- Trends in
  - Digital technologies
  - Security threats
- Opportunities in 2018
- Questions



Disclaimer: presentation reflects my personal views and not perse that of my employer

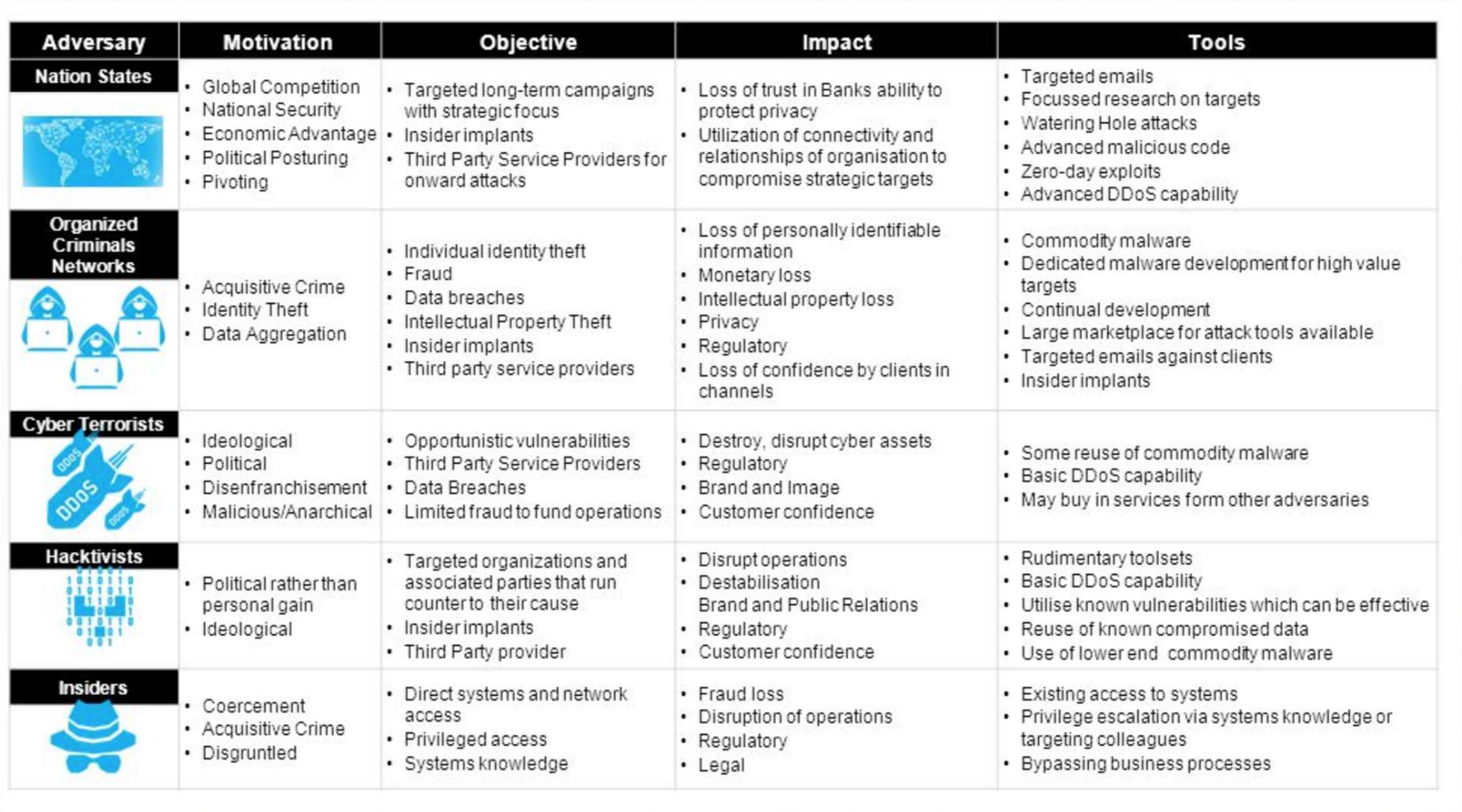
A bit about myself

- CISO - International Atomic Energy Agency (IAEA) since 2015
- Previously working:
    - CISO - Organisation for the Prohibition of Chemical Weapons (OPCW)
    - Information and IT Security Consultancy
    - IT Security Systems implementer and project manager
    - IT System Administrator
- Academic background in Computer Science and Astronomy
- Wife, 4 children (3 girls) and a (female) cat in NL

Impact of digital technology on society

(Negative) Results

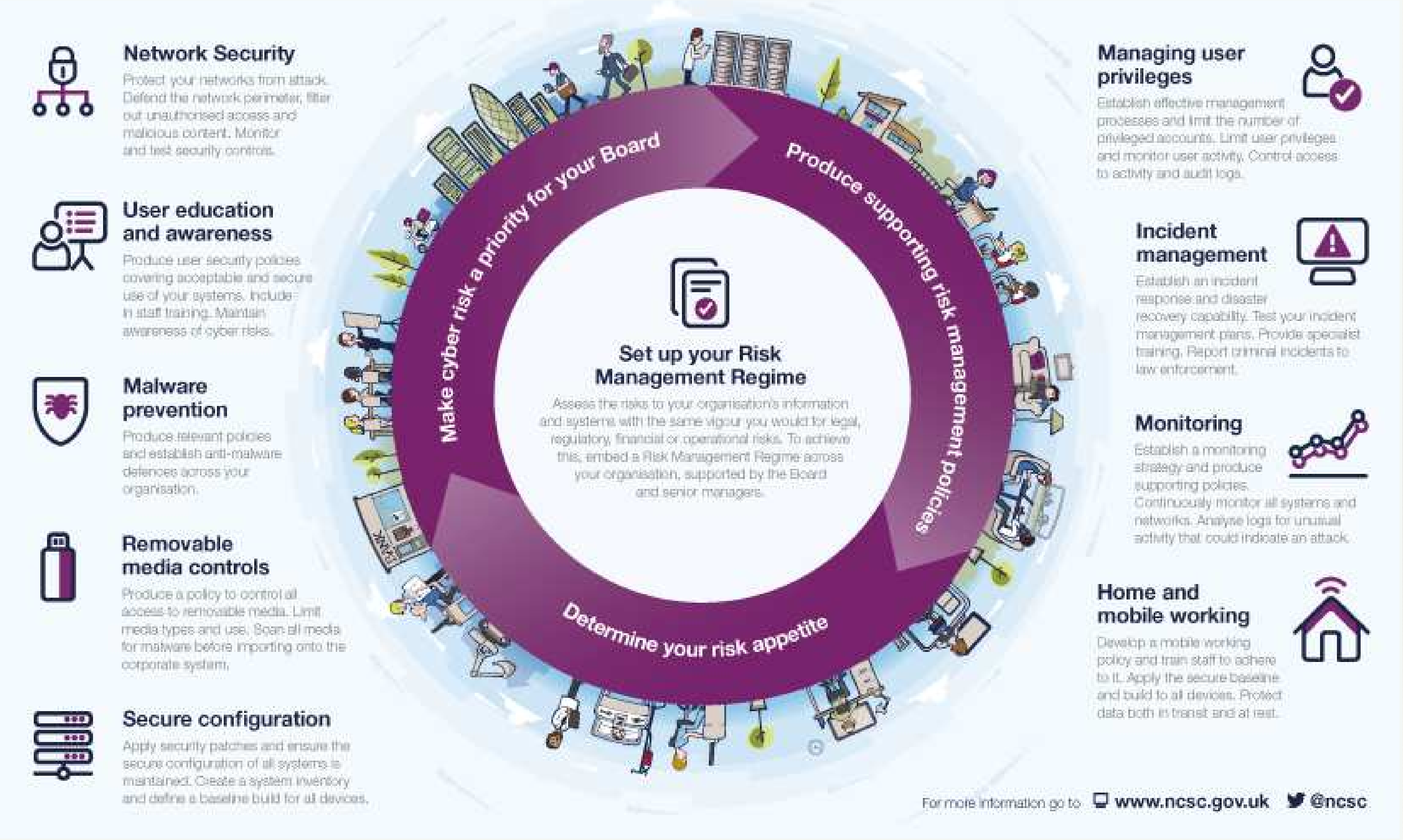
Cyber Adversaries



Adversary	Motivation	Objective	Impact	Tools
Nation States	• Global Competition • National Security • Economic Advantage • Political Posturing • Pivoting	• Targeted long-term campaigns with strategic focus • Insider implants • Third Party Service Providers for onward attacks	• Loss of trust in Banks ability to protect privacy • Utilization of connectivity and relationships of organisation to compromise strategic targets	• Targeted emails • Focussed research on targets • Watering Hole attacks • Advanced malicious code • Zero-day exploits • Advanced DDoS capability
Organized Criminals Networks	• Acquisitive Crime • Identity Theft • Data Aggregation	• Individual identity theft • Fraud • Data breaches • Intellectual Property Theft • Insider implants • Third party service providers	• Loss of personally identifiable information • Monetary loss • Intellectual property loss • Privacy • Regulatory • Loss of confidence by clients in channels	• Commodity malware • Dedicated malware development for high value targets • Continual development • Large marketplace for attack tools available • Targeted emails against clients • Insider implants
Cyber Terrorists	• Ideological • Political • Disenfranchisement • Malicious/Anarchical	• Opportunistic vulnerabilities • Third Party Service Providers • Data Breaches • Limited fraud to fund operations	• Destroy, disrupt cyber assets • Regulatory • Brand and Image • Customer confidence	• Some reuse of commodity malware • Basic DDoS capability • May buy in services form other adversaries
Hacktivists	• Political rather than personal gain • Ideological	• Targeted organizations and associated parties that run counter to their cause • Insider implants • Third Party provider	• Disrupt operations • Destabilisation Brand and Public Relations • Regulatory • Customer confidence	• Rudimentary toolsets • Basic DDoS capability • Utilise known vulnerabilities which can be effective • Reuse of known compromised data • Use of lower end commodity malware
Insiders	• Coercement • Acquisitive Crime • Disgruntled	• Direct systems and network access • Privileged access • Systems knowledge	• Fraud loss • Disruption of operations • Regulatory • Legal	• Existing access to systems • Privilege escalation via systems knowledge or targeting colleagues • Bypassing business processes

Results on Cyber Security

Elements of Cyber Security


Make cyber risk a priority for your Board
Produce supporting risk management policies
Determine your risk appetite

Network Security

Protect your networks from attack. Defend the network perimeter, filter out unauthorised access and malicious content. Monitor and test security controls.

User education and awareness

Produce user security policies covering acceptable and secure use of your systems. Include in staff training. Maintain awareness of cyber risks.

Malware prevention

Produce relevant policies and establish anti-malware defences across your organisation.

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 onto the corporate system.

Secure configuration

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

Set up your Risk Management Regime

Assess the risks to your organisation's information and systems with the same vigour you would for legal, regulatory, financial or operational risks. To achieve this, embed a Risk Management Regime across your organisation, supported by the Board and senior managers.

Managing user privileges

Establish effective 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 recovery capability. Test your incident management plans. Provide specialist training. Report criminal incidents to law enforcement.

Monitoring

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

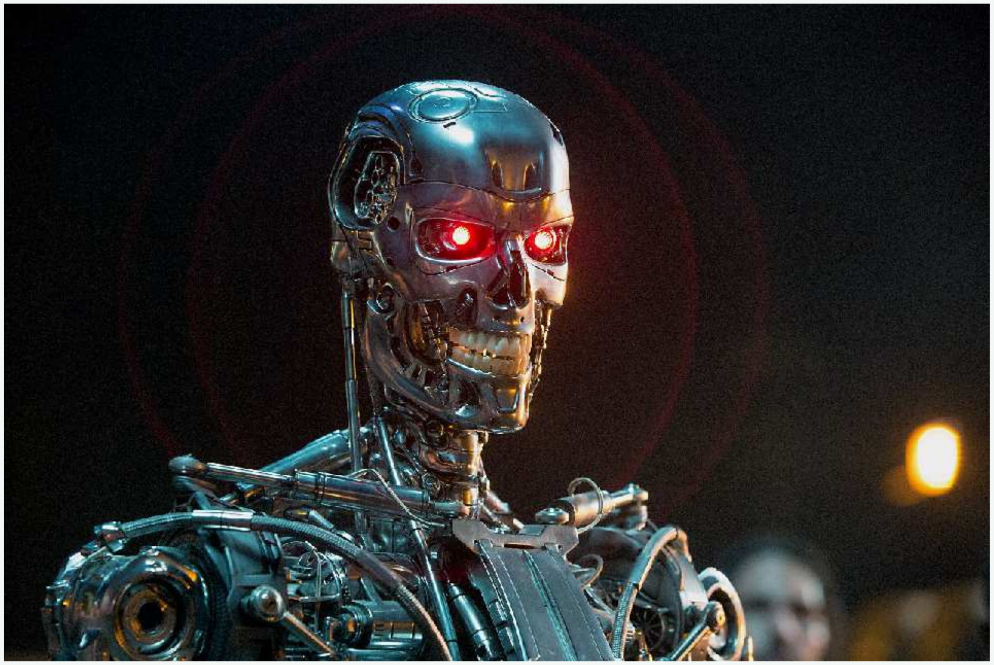
Home and mobile working

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

For more information go to www.ncsc.gov.uk @ncsc

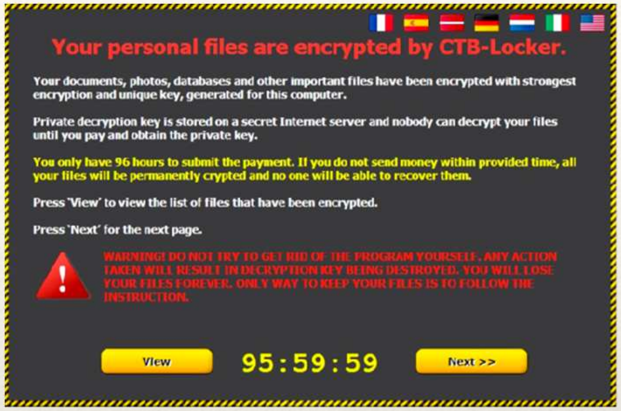
IT Trends 2018 onwards

- Artificial Intelligence
- Voice & visual search
- Virtual & Augmented reality
- Crypto currencies & Distributed ledgers
- Internet of Things (IoT)



Cyber Security Threat Trends

- Ransomeware
- Hacking IoT devices
- Financial trojans targeting financial institutions
- Mobile threats growing
- Social media as an attack vector
- Attacks industrial / IoT devices will grow
- Increased state level involvement
- Attribution will become harder



Your personal files are encrypted by CTB-Locker.

Your documents, photos, databases and other important files have been encrypted with strongest encryption and unique key, generated for this computer.

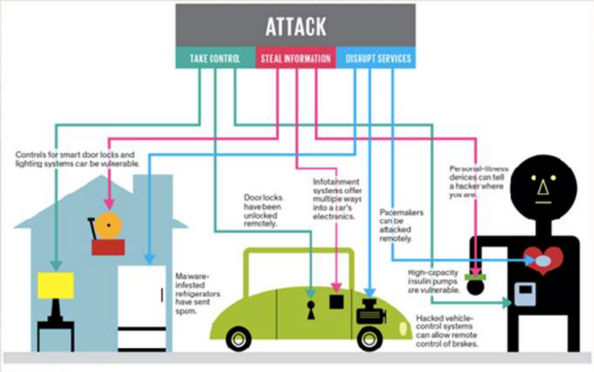
Private decryption key is stored on a secret Internet server and nobody can decrypt your files until you pay and obtain the private key.

You only have 96 hours to submit the payment. If you do not send money within provided time, all your files will be permanently crypted and no one will be able to recover them.

Press 'View' to view the list of files that have been encrypted.

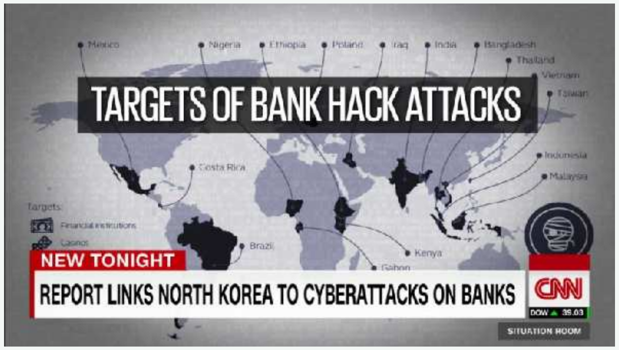
Press 'Next' for the next page.

WARNING! DO NOT TRY TO GET RID OF THE PROGRAM YOURSELF. ANY ACTION TAKEN WILL RESULT IN DECRYPTION KEY BEING DESTROYED. YOU WILL LOSE YOUR FILES FOREVER. ONLY WAY TO KEEP YOUR FILES IS TO FOLLOW THE INSTRUCTION.



ATTACK
TAKE CONTROL
STEAL INFORMATION
DISRUPT SERVICES
Controls for smart door locks and lighting systems can be vulnerable.
Door locks have been unlocked remotely.
Infotainment systems offer multiple ways into a car's electronics.
Pacemakers can be attacked remotely.
Personal-fitness devices can tell a hacker where you are.
Malware-infested refrigerators have sent spam.
High-capacity insulin pumps are vulnerable.
Hacked vehicle-control systems can allow remote control of brakes.

Illustration: J. D. King



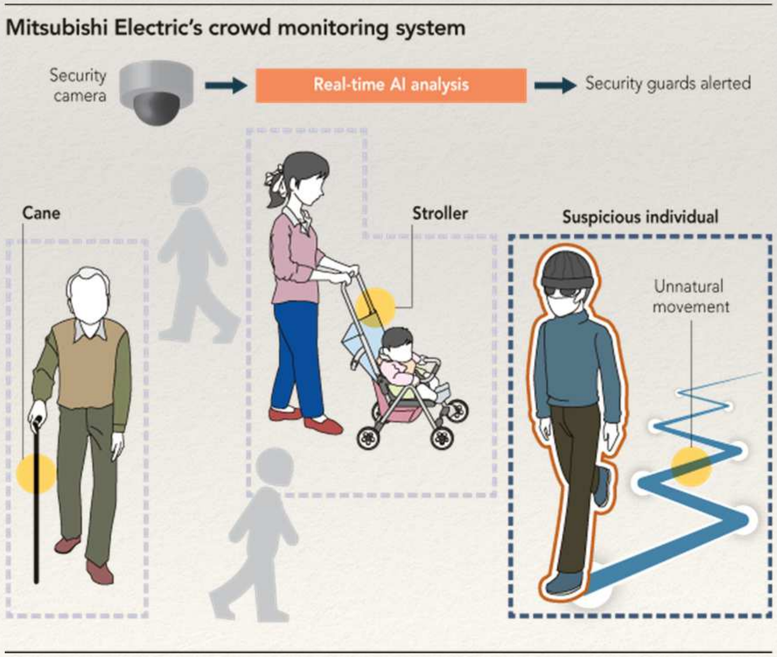
TARGETS OF BANK HACK ATTACKS

NEW TONIGHT

REPORT LINKS NORTH KOREA TO CYBERATTACKS ON BANKS

2018 Opportunities for Security

- Improving security hygiene (100%)
- EU General Data Protection Regulation (GDPR) - Privacy
- Artificial Intelligence (AI)
- Abstraction from IT infrastructures
- Focus on Risk Management


Mitsubishi Electric's crowd monitoring system

Conclusion

- Impact and dependancy of digital technologies keeps growing
    - New applications as never seen before
    - Disruption of traditionally closed markets
- Increased necessity for security will show in high demand for talent
- Improved opportunities for females as IT and IT security moves away from hardcore technology

Any Questions