MOSAIC™

Financial Services Infrastructure

Security awareness – Cyber/Physical

Ref ISMS202108

Objectives

- Increase awareness of security
  - Develop a security conscious culture
- Understand why security is important
- What are we doing
- Identify (some) security threats

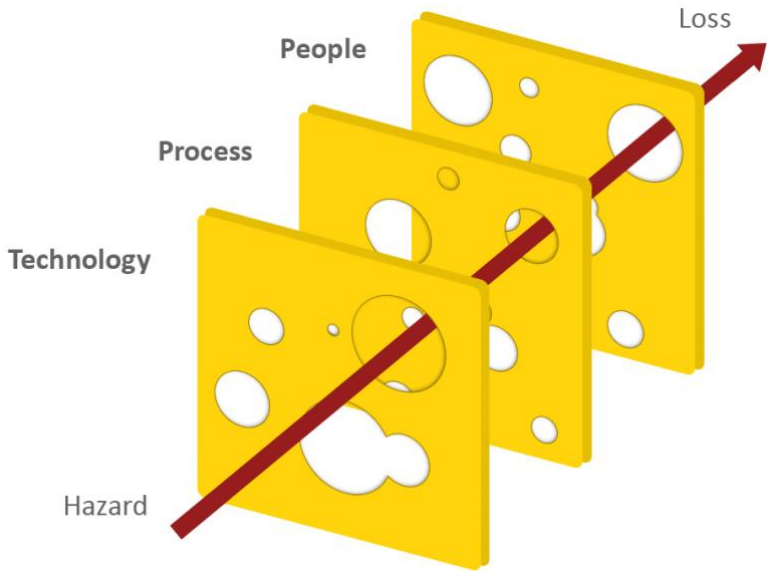
Agenda

- What is cyber/physical security ?
- What is Phishing ?
- Why is security important ?
- Where are some of the threats coming from ?
- What assets are we protecting ?
- How big is the threat ?
- What can we do ?
- Next Steps

What is cyber security ?

"I don't know who those Cybers are, but I'm ready for their attack!"

What is cyber security ?



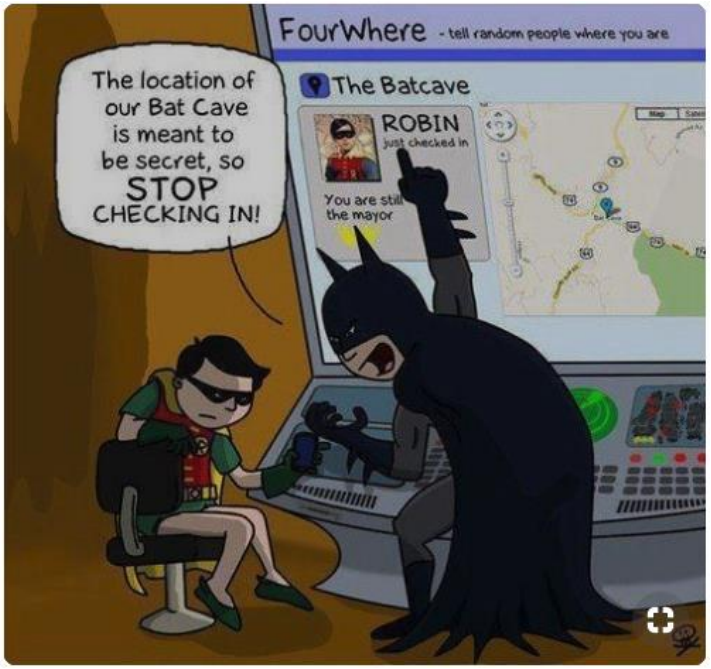
What is cyber security ?

- “Cyber security comprises technologies, processes and controls that are designed to protect systems, networks and data from cyber attacks.
- Effective cyber security reduces the risk of cyber attacks and protects organisation and individuals from the unauthorised exploitation of systems, networks and technologies.”

What is Phishing ?

- Phishing is a method used to compromise the computers of and steal sensitive information from individuals by pretending to be an email from or the website of a trusted organisation.
- The goal is to trick the email recipient into believing that the message is something they want or need, such as a request from their bank, or a note from someone in their company.
- What distinguishes phishing is the form the message takes, the attackers masquerade as a trusted entity of some kind, often a real or plausibly real person, or a company the victim might do business with.
- All it takes is one employee to take the bait.

Why is cyber security important to us ?



Why is cyber security important (to us) ?

- Smartphones, tablets and laptops have also made it easier for hackers and fraudsters to be successful.
- Android and Apple applications are an easy target as they are mostly unregulated and can hit many users quickly under disguise as a legal application.
- McAfee (2016) identified over 37 million malware-installed applications across both Apple and Google's app stores during the last six months of 2015 alone.
- Cloud storage, such as Dropbox, is also being targeted by hackers because individuals and corporations store sensitive and valuable information that can be easily compromised and stolen.
- As well as individual consumers, there are also major cyber threats to business as highlighted in the NCA cyber threat to business 2017- 2018 report.
- The report highlighted significant incidents including ransomware and distributed denial of service attacks, massive data breaches, supply chain compromises, fake news and information operations, CEO/business email compromise fraud, significant security vulnerabilities and financial sector compromise.

Why is cyber security important (to us) ?

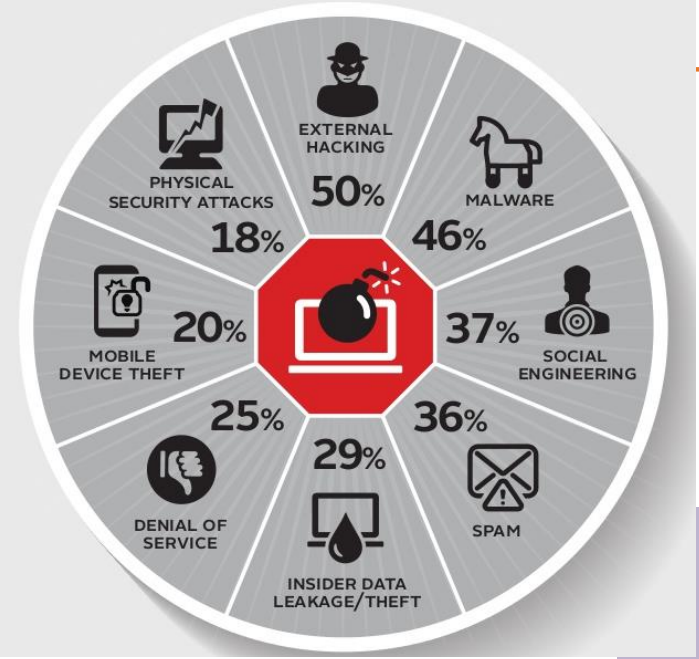
- Due to this increase risks cybersecurity is essential to Mosaic FSI too:

1. Protects our customers.
2. Protects Mosaic.
3. Contractually obligated to meet specific standards, i.e., ISO27001.
4. Practice what we preach and deliver.
5. Good practice in business and personal lives.
6. Awareness and vigilance are critical given global growth of Cyberattacks.

What assets are we protecting ?

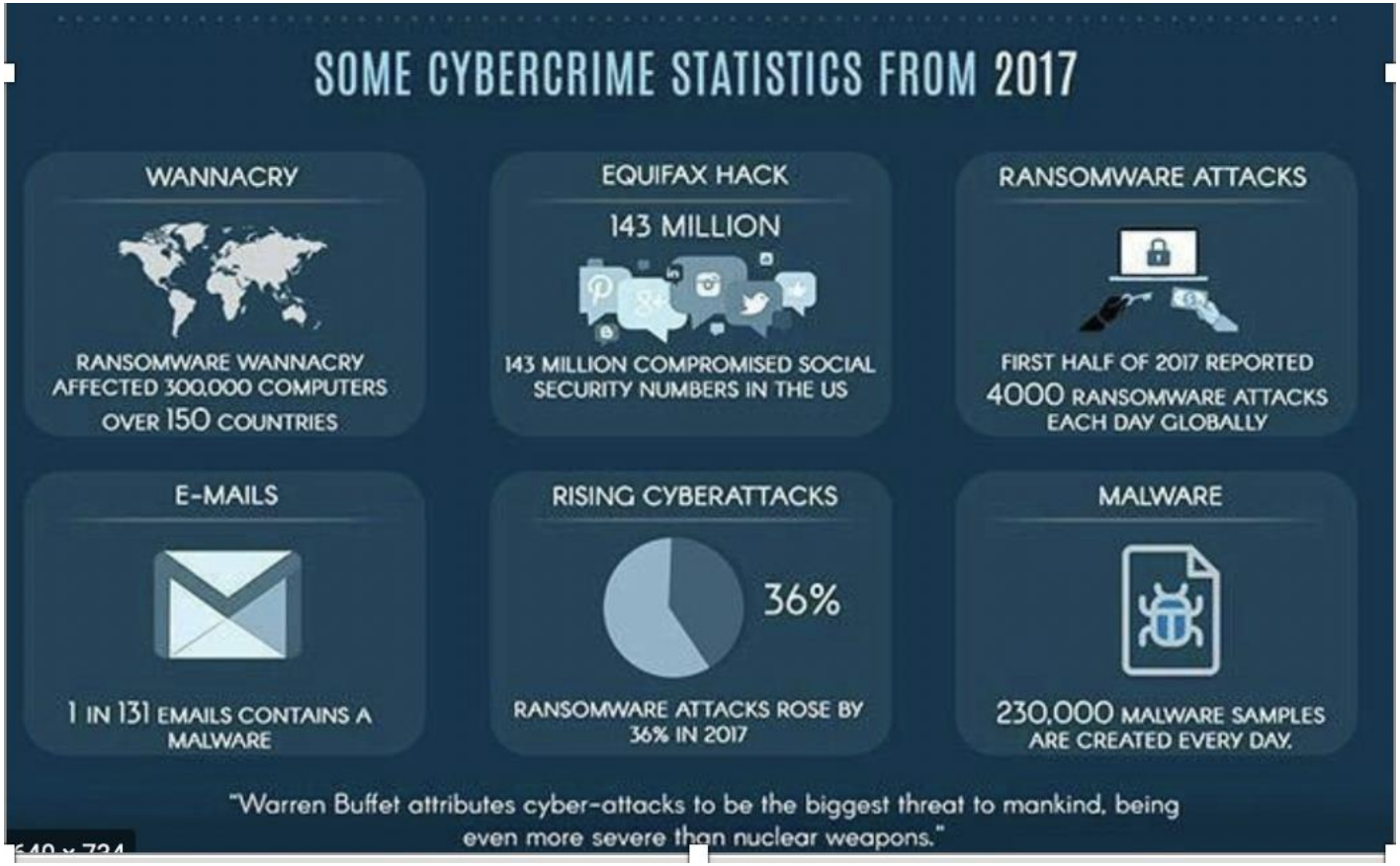
- Customers
  - Information & data
  - Their customers information & data
  - Strategic initiatives from M & A to NPD
  - Brand and reputation
  - Other?
- Mosaic
  - Our reputation and brand
  - Your personal reputation
  - Our ability to operate as a business
  - Other?

Where are the threats coming from ?

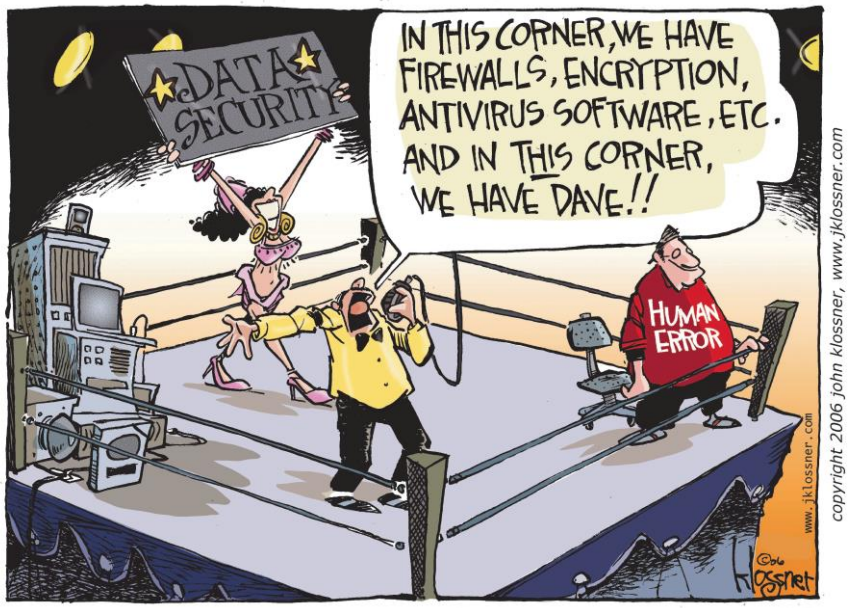


MOSAIC™ Financial Services Infrastructure

How big is the threat



What can we do ?



What can we do ?

- Cyber awareness/prevention must be our cultural ‘modus operandi”
- Do the basics really well!!
  - Always lock your device when unattended
  - Never take customer data outside of approved locations
  - Respect client IP and NDA’s
  - Do not use company laptops for personal use
  - Never share your password
  - Never share your laptop
  - Protecting physical data is just as important as electronic data
  - Do not print customer project information unless absolutely necessary and/or customer approved
  - Change passwords regularly and utilise TFA where ever possible
- Be constantly vigilant to any form of attack, assertively push back on colleagues, customers, friends or other who willingly or unwillingly encourage the wrong type of behaviour

What can we do - Phishing ?

- Deploy a spam filter that detects viruses and blank senders
- Use Two-factor authentication
- Enabled browser add-ons and extensions on browsers that prevent users from clicking on malicious links.
- Keep all systems current with the latest security patches and updates.
- Install an antivirus solution, schedule signature updates, and monitor the antivirus status on all equipment.
- Make sure you have read the Mosaic FSI Information security policy and Mosaic FSI Information security management System (ISMS)
- Deploy a web filter to block malicious websites.
- Encrypt all sensitive company information.
- Convert HTML email into text-only email messages or disable HTML email messages.

Be aware of malicious links in emails before clicking on any links:

1. Check the email address for example if it is coming from a utility company, then the email address is not going to be a Gmail or Hotmail address.
2. If the domain inserted into the link does not match the company domain, then the link is a fake.
3. If you still have a suspicion go with your instinct and do not click on the link, if you have been waiting on the information you can always ring the company and check that the email came from them.

What have we got

ISO 27001 documents

ISMS, information security policy, ISO 27001 statement of applicability, ISO 27001 risk assessment methodology including appendix 1 – risk assessment table spreadsheet and appendix 2 – risk treatment table spreadsheet, IT and social media policy including social media threats awareness, cyber security and phishing awareness, data protection policy including data privacy awareness, data breach notification plan, business continuity plan, disaster recovery plan, internal audit checklist and internal audit report.

Human Resource Privacy Documents

Confidentiality agreement, consent form for new employees uses of data, consent form for unsuccessful job applicants, consent form for the use of data for existing employees, consent form for employees who is leaving, AML onboarding policy and Anti-Bribery policy.

Purchasing

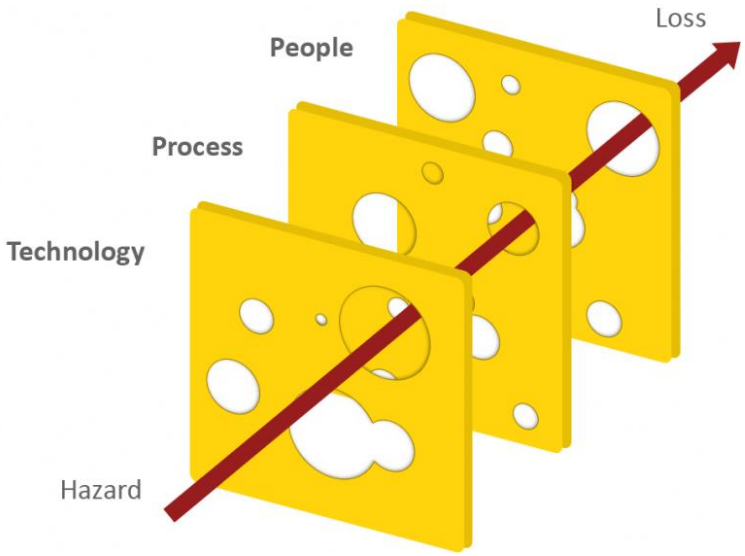
Supplier Assessment

Record Keeping

Records retention and protection policy, Mosaic FSI security log and document control procedure.

What can we do ?

- “No major accident has ever been caused by a single error alone”



MOSAIC™ Financial Services Infrastructure

What are and can we do?

- Whatever we do we can’t identify all of the risks let alone mitigate them.
- Strategy
  - Basics first
    - Passwords, encryption, email/web practices, training
  - Develop a solid foundation
    - Culture, training, virus protection, TFA,
  - Common sense = common practice
  - Remain vigilant
  - Report a breach to security officer (M Stobbs)