CYBERSECURITY: Regional Challenges

Presenter : Althea C Bartley

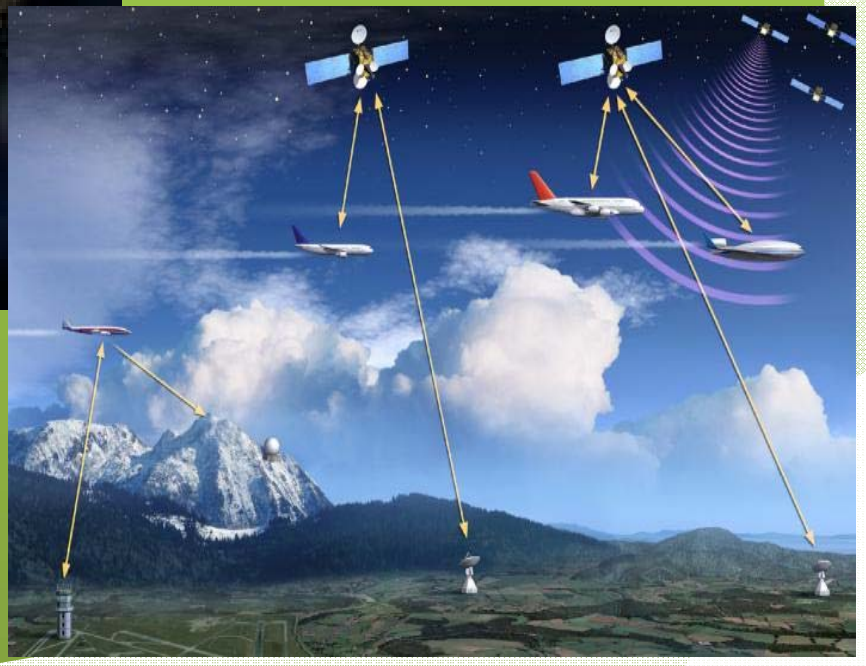
Manager Aviation Security & Facilitation

Cybersecurity: Regional Challenges

- Aviation Security and the Digital Age
- Are we prepared as a Region?
- Moving Forward – Managing Cyber Risks

Aviation Security in the Digital Age

Increased use of information technology means greater exposure to cyber attacks.



NextGen will move the air transport system to satellite based surveillance instead of ground based radar

Are we prepared as a Region?

- Vulnerabilities in the Aviation Industry

In 2010 two years after Spanair accident it was revealed that the central computer system used to monitor technical problems in the aircraft was infected with malware.

Aviation Security and the Digital Age

Reduction of manpower and increase use of IT to reduce cost and increase efficiency

Airports and airlines facilitating the IT savvy passenger by facilitating the use of e-ticking and immigration kiosks

Are we prepared as a Region?

- Vulnerabilities in the Aviation Industry

July 2013 Istanbul Ataturk and Sabiha Gokcen International Airport were victims to a malware attack as cybercriminals attempted to steal data from the airports passport control system.

Are we prepared as a Region?

March 2015 British Airways freezes frequent flyer programme due to an automated computer program looking for vulnerabilities in their security systems

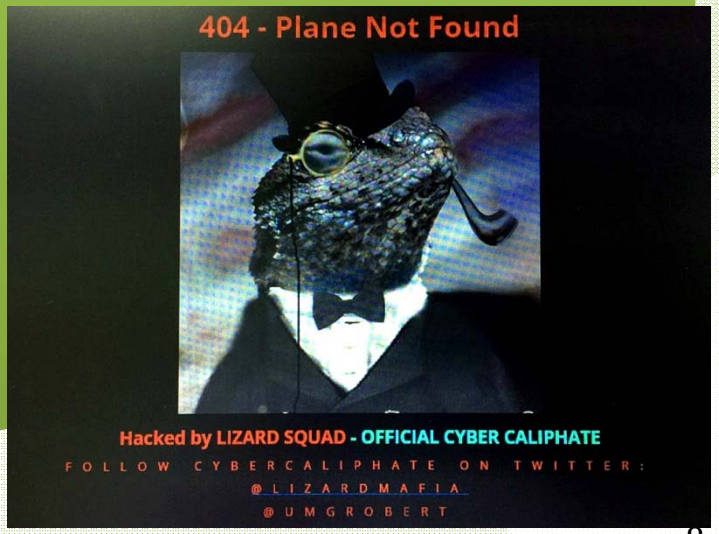
September 2013 Japan Airlines reports that f up to 750,000 of its miles program customers personal information had been compromised due to a cyber attack.

Are we prepared as a Region?

- Vulnerabilities in the Aviation Industry

March 2014 Malaysia Civil Aviation was hacked a day after the report of MH370 via email as a PDF document

January 2015 Malaysia Civil Aviation Website was hacked the Lizard Squad.

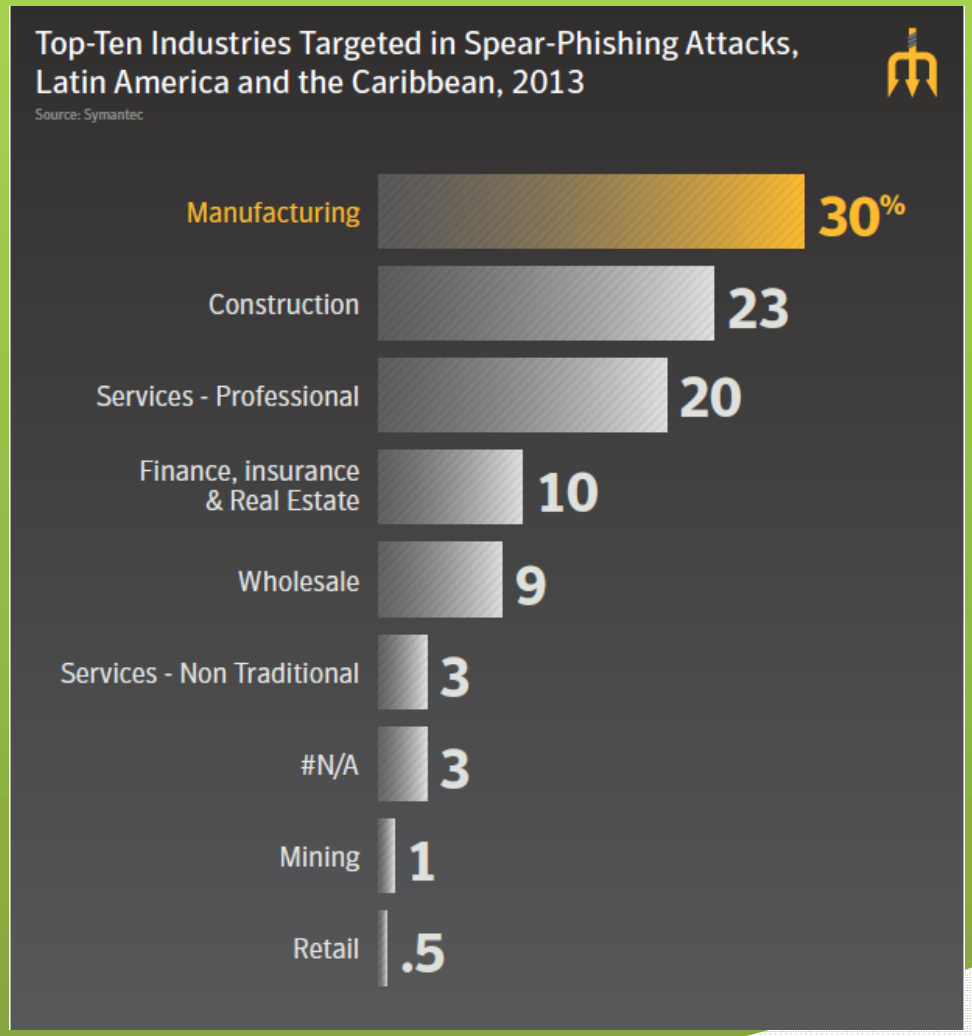


Are we prepared as a Region?

- Vulnerabilities in the Aviation Industry

November 2014 over 10 government websites to include Jamaica Civil Aviation Authority were the target of a "Denial of Service" attack

Are we prepared as a Region?



TARGETED ATTACK

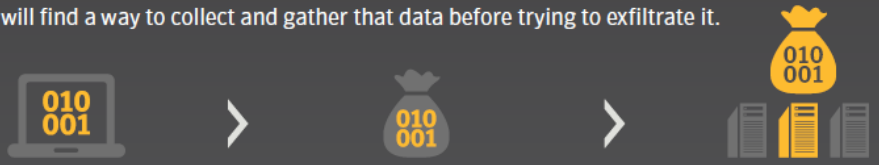
KEY STAGES

Source: Symantec

01 INCURSION The attacker gains entry to the targeted organization. This is often preceded by reconnaissance activities where the attacker is looking for a suitable social engineering tactic.

02 DISCOVERY Once the attacker has gained entry, they will seek to maintain that access as well as discover what data and other valuable resources they may wish to access.

03 CAPTURE Once the valuable data has been discovered and identified, the attacker will find a way to collect and gather that data before trying to exfiltrate it.



04 EXFILTRATION The attacker will find a mechanism to steal the data from the targeted organization. This may be by uploading it to a remote server or website the attackers have access to. More covert methods may involve encryption and steganography, to further obfuscate the exfiltration process, such as hiding data inside DNS request packets.

Moving Forward- Managing Cyber Risk

CANSO Recommends:

- Conduct Risk Assessment
- Adopt a proactive approach to cybersecurity
- Security Culture
- Training and Awareness
- Monitoring and Reporting

Moving Forward- Managing Cyber Risk

ICAO AVSEC Panel:

Not just ATM systems

- Airport Operations
- Airport Security Systems
- Airline Systems
- And others

Moving Forward- Managing Cyber Risk

- Develop a Cyber Security Strategy
  - Industry Awareness
  - Legislative and Regulatory Framework
  - Identify Resources available to build capacity
  - Information sharing between Regulator, Industry and relevant agencies


HACKER
ATTACK
CYBER
NETWORK
TERRORISM
GROUPS
TARGET
INTERNET
CRIME
HACKING
COMPUTER
CRIMINAL
HACKERS
INFORMATION
SYSTEM
DEPARTMENT
SERVICES
SYSTEMS
DEVICES
PORNOGRAPHY
OFFENSIVE
INDIVIDUALS
WEBSITES
USED
ACTIVITIES
DATA
SENDING
COMMITTED
FINANCIAL
ALLEGEDLY
CHILD
HARASSMENT
ALTERING
IDENTITY
UNAUTHORIZED
NEEDED
MAIL
WARFARE
ACCESS
USING
COMMUNICATIONS
NETWORKS
INTERNATIONAL
SERVICE
THEFT
CONTENT
ILLEGAL
INVESTIGATORS
ROOMS
BOTNET
ELECTRONIC
LIMITS
REFERS
UNSOLICITED
DEROGATORY
COPYRIGHT
ORGANIZED
FUTURE
FEDERAL
ENCRYPTED
GOVERNMENT
CASES
FRAUD
OFFICIALS
JURISDICTIONS
MILLION
COMPANIES
DEFENSE
CYBERTERRORISM
OBSCENE
INCLUDING
SERVER
DOCUMENT
RACE
RING
CAUSE
INCLUDE
DOCUMENTED
PROBLEMS
RESOURCES
SPECIFIC
INFECTED
PEOPLE
MAIN
MAJOR
FACE
MALICIOUS
TECHNOLOGY
USE
DRUG
DISTRIBUTED
INDIVIDUAL
UNIVERSITY
HIGH
INCREASINGLY
TRAFFICKING
STORED
FACILITATED
TECHNICAL
CONSIDERED
DIRECTLY
BETWEEN
DURING
COMBATTING
WEBSITE
VARIETY
GROUP
CONCERN
CODE
HARM
VICTIM
PHYSICAL
HATE
TRAFFICKERS
SECURITY
SEVERAL
TIME
GOING
CYBERSPACE
WELL
SCAMS
KINETIC
TRADES
DETECT
ADVANCE
PURPOSES
SPAM
FORM
WAY
NATION
AREA
SURROUNDING
TOPOLOGY
STALKING
COUNTS
ENTERING
DEFINED
PACKAGES
INCLUDED
CITATION
UNLAWFUL
PROFILE
SPECIFIC

Thank You