canso

civil air navigation services organisation

Transforming Global ATM Performance

Cybersecurity the new challenge

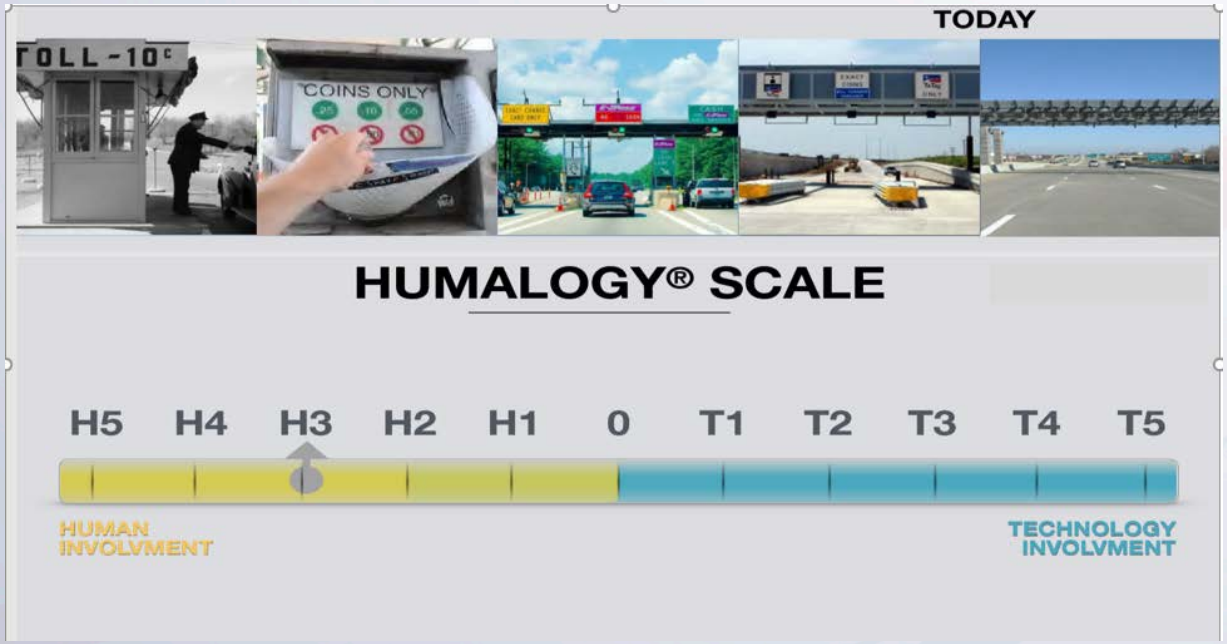
Antonio Palacios

CEO, Telnorm Teltech

Regulatory Framework

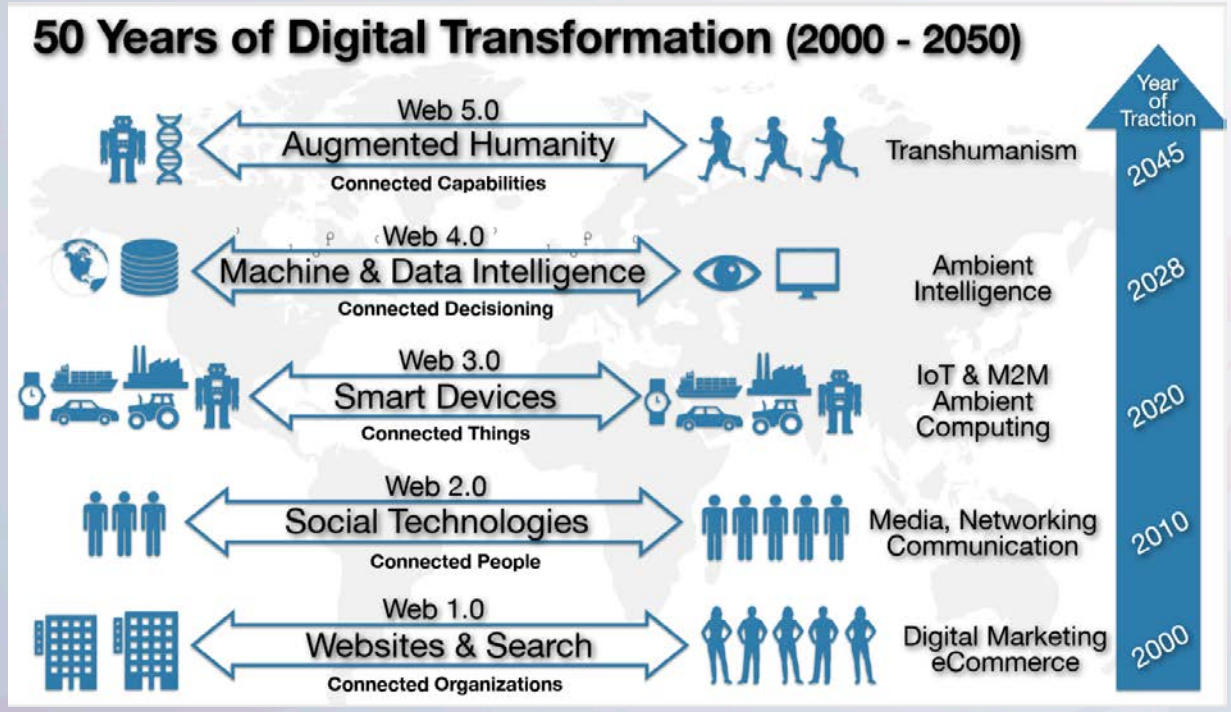
- ICAO Aviation Security Manual Annex 17
- NIST Cybersecurity Framework
- European Union Agency for Network and Information Security (ENISA) and repealing Regulation (EC) No 460/2004
- FAA Cybersecurity Roles and Responsibilities 1370.47
- ISO 27000 Series of Standards

Digital Transformation



So where is security in this scale ?

Digital Transformation



Cybersecurity Risk Grows

- Augmentation
  Extortion/Control
- MI Extortion/Corruption
- Device Takeover
- Social Engineering
- Viruses


95%
Of all successful cyber attacks are caused by human error
Source: IBM Cyber Security Intelligence Index

The Golden edge for Data Exploits

Growth in Information

Growth in Devices

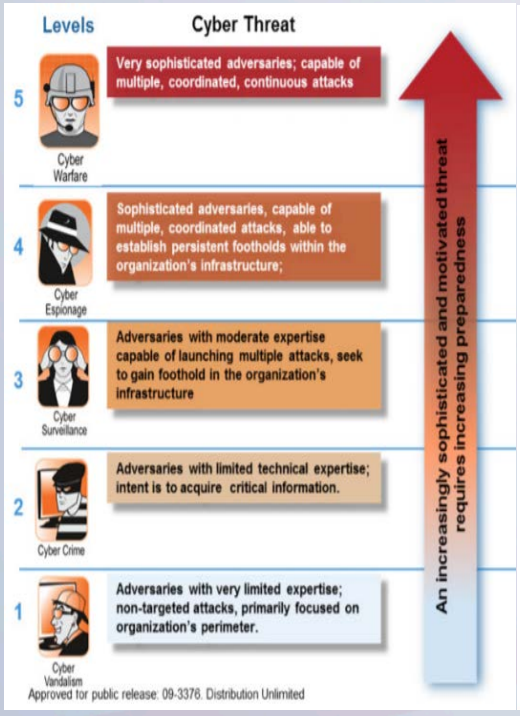
Growth in Software

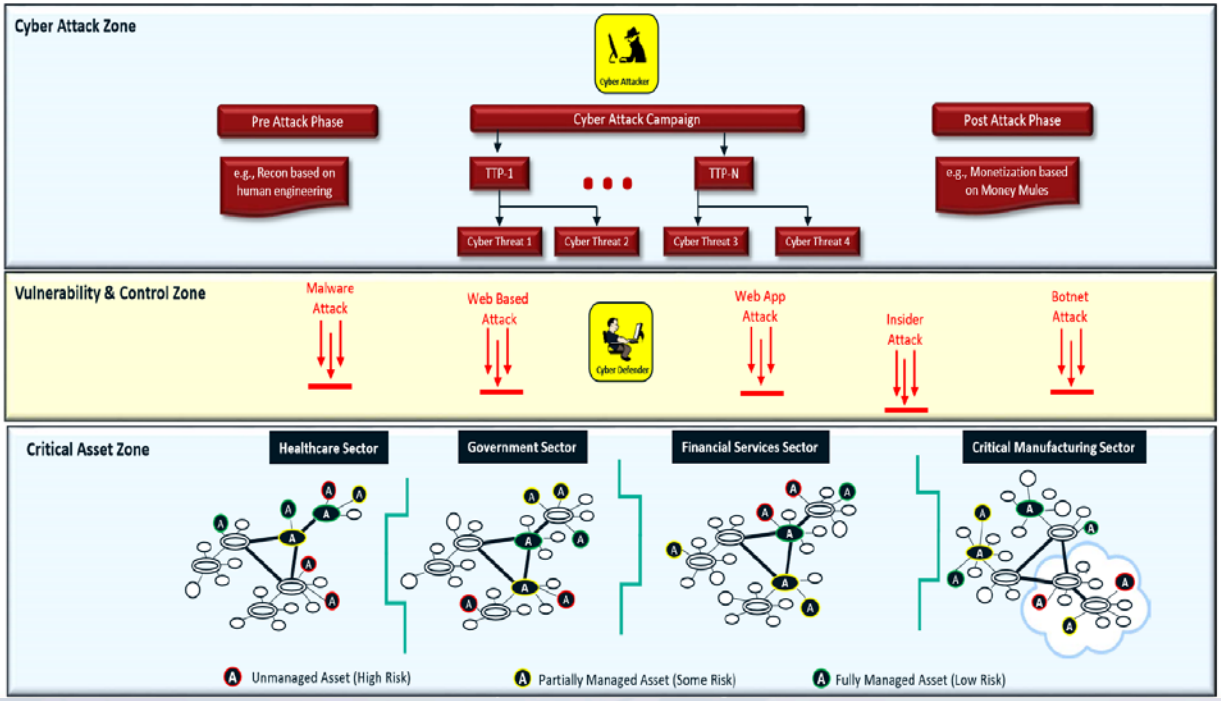
Growth in Cloud

Growth in Outsourcing

Growth in Threats

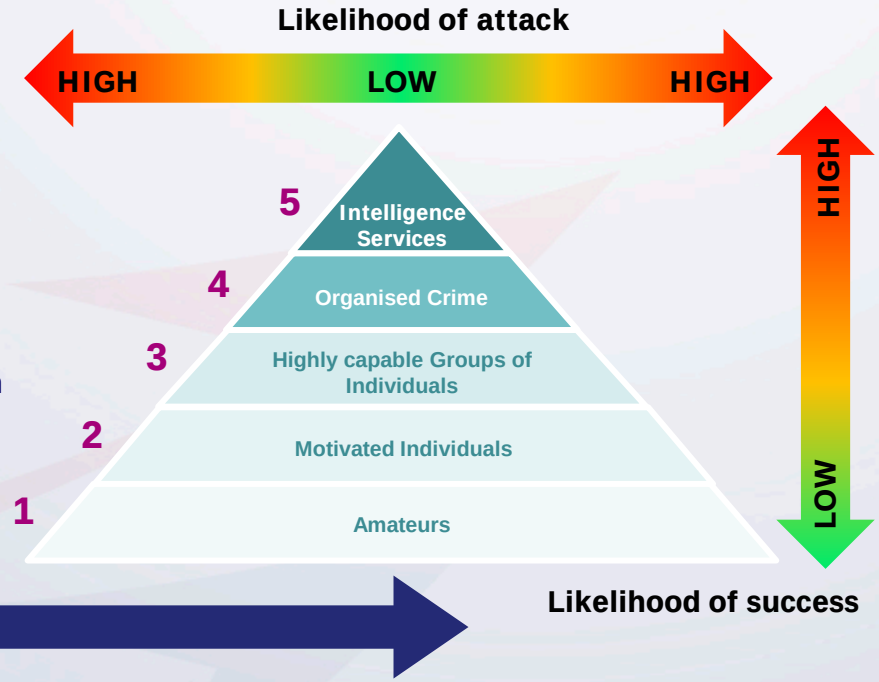
Cyber Threat landscape





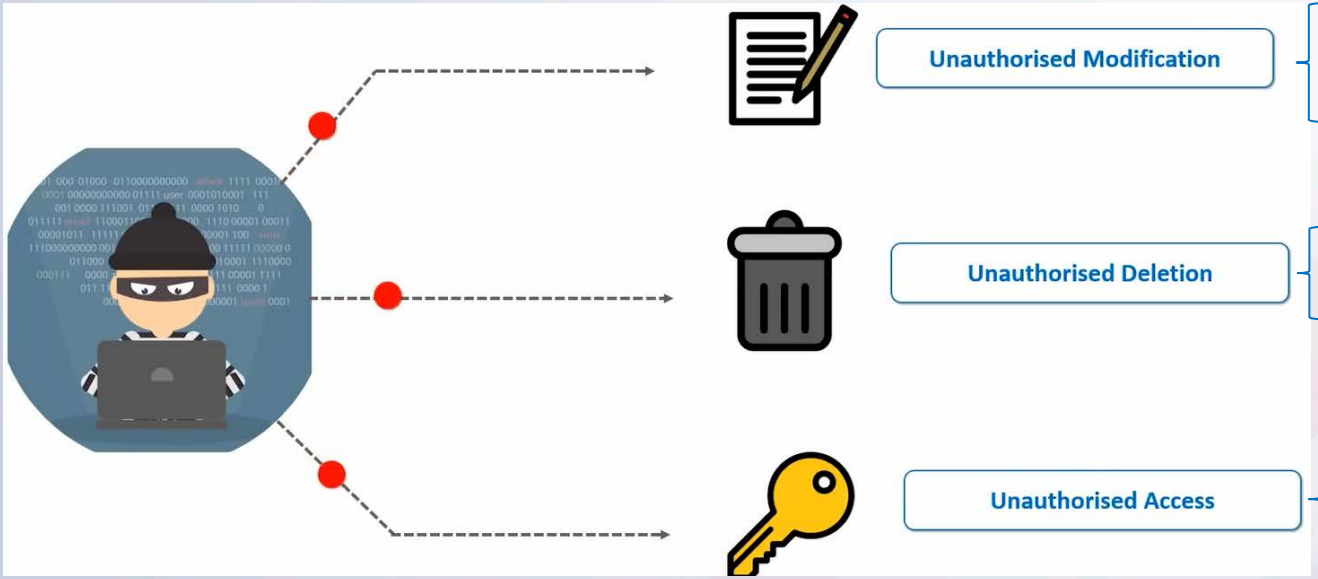
General Trend in Cyber-Threat

- Insider Threat including inadvertent action(s) which involves individual(s) with access to organizations' systems continues to hold top place with roughly 55 % of the attacks
- Outsider threat is responsible for roughly 45 % of the attacks
- Targeted attacks which hints very intentional acts and sophistication are often against State's Critical Infrastructure Systems : ANSP classification in many Countries
- Untargeted attacks continue to be most common and widespread malicious actions



Air Gap is not enough

Protect Against What



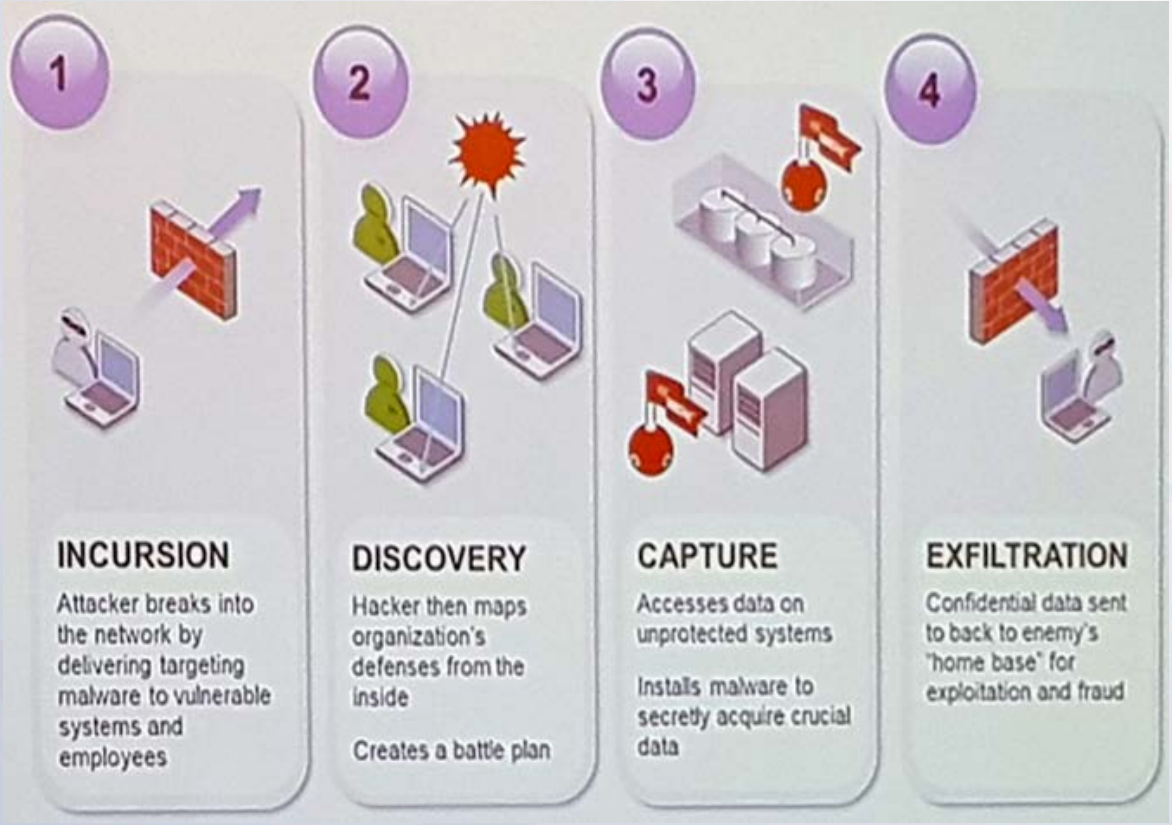
- Integrity
- Authentication
- Non.Repudiation

- Integrity
- Availability

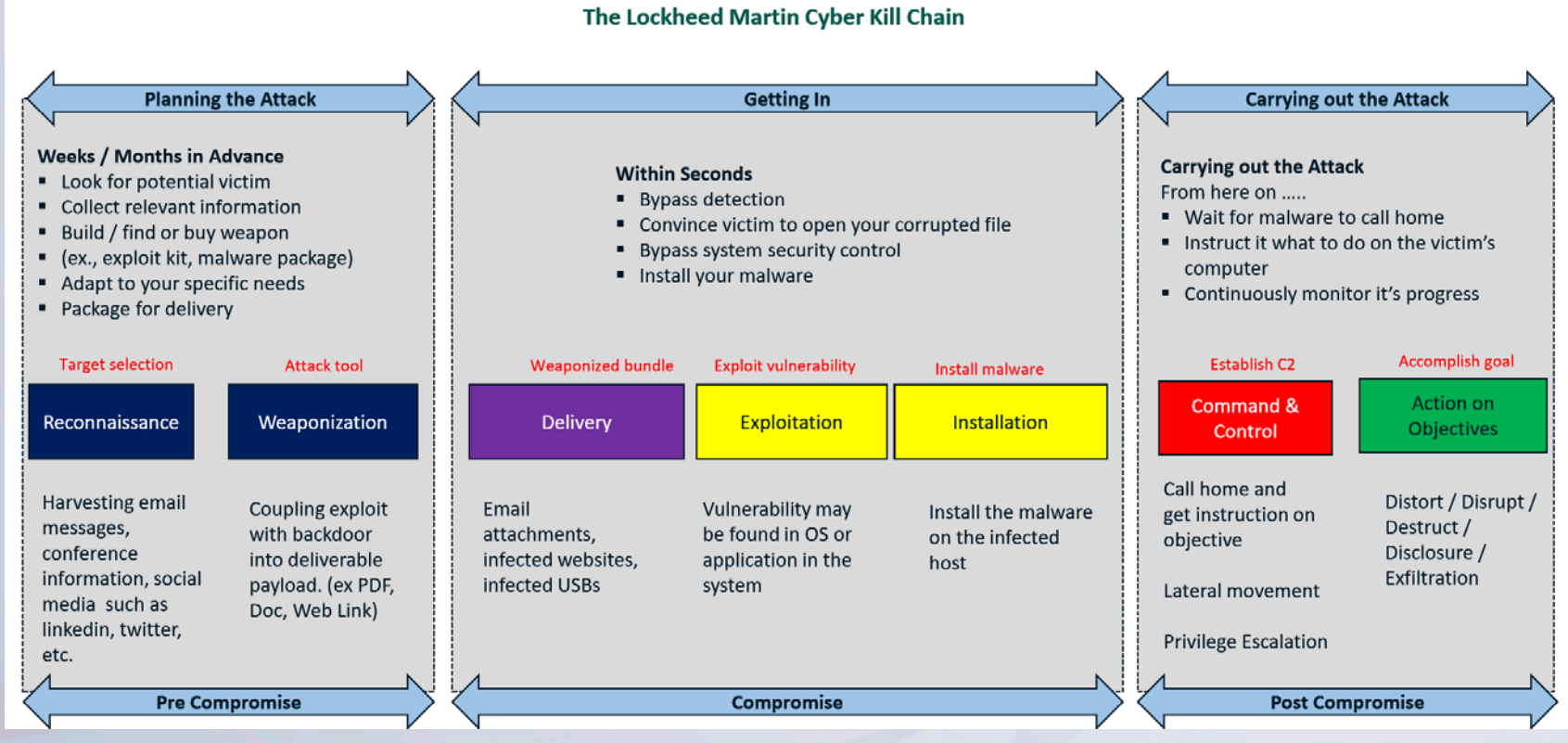
- Confidentiality
- Authorization
- Traceability

Cyber Threats

How Targeted Attacks Work



Understanding Cyber Attacks



Everybody is Vulnerable

- 9/21/18- Romanian woman pleads guilty to ransomware attack on D.C. police cameras before Trump Inauguration
- 9/12/18- No fly-by-night operation: Researchers suspect Magecart group behind British Airways breach
- 9/12/18- Canadian town bows to ransomware attack, will pay attackers
- 9/6/18- Patched bug could have allowed attackers to remotely disconnect PLC devices from ICS systems
- 8/16/18- Chinese hackers targeted US firms after trade mission
- 7/23/18- Russian hackers penetrated networks of US electric utilities
- 6/28/18- China's penetration of Silicon Valley creates risks for startups (think CFIUS and new ways for China to get access to US IP)
- 6/19/18- China based campaign breached satellite, defense companies

Transportation Security

- 9/15/18- Tesla stolen via cell phone at the Mall of America, Tesla has a “bug” bounty program.
- 9/25/17- Stealing cars via keyless entry system
- 2015- Hackers take control of a Jeep Cherokee via the car’s Uconnect system resulting in the recall of 1.4 millon vehicles.
- What about a Stuxnet type attack on vehicles…

Ransomware Update

- SamSam Hits Atlanta March 2018
  - The court system cancelled appointments
  - 90% of computers at the Dept of Public Works were inaccessible
  - Years of dash cam video captured by police was lost
  - Cost them $17m to date
    - $51,000 was the ransom

Cyber-Attacks are Multiplying in Many Sectors

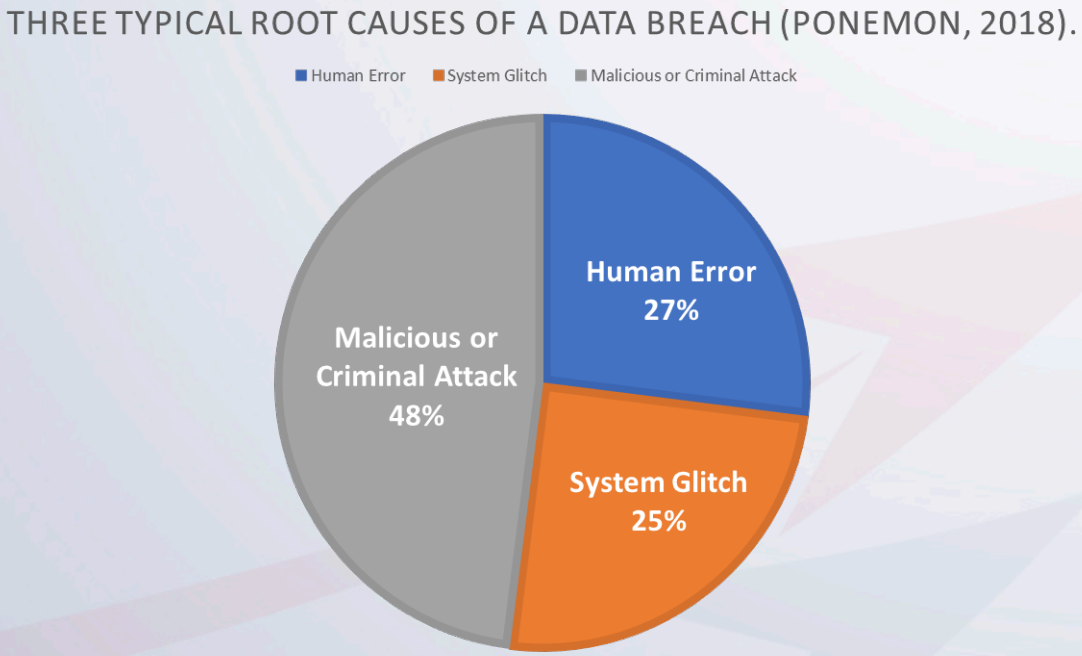
In 2016 more than 60 new ransomwares appeared
(Source SANS)

67% of enterprises have now been breached

+250 M€ Estimated cost of the 2017 “Not Petya” attack for one company

- Cyberwar & “destructive” attacks: Ukraine power grid attack, TV5 Monde, …
- Denial of Service attacks : Boryspil Airport (Kiev Ukraine), Indonesian Airlines and Airports (to protest against Air pollution), Hanoi Ho Chi Minh Airports, …
- Information theft: Operation Cleaver - Pakistan, Qatar, Korean airlines, …
- Ransomware: Hospitals, Civil Aviation Authorities, ...

Data Breach Update



Aviation & ATM becomes more exposed

Attack surface & vulnerabilities are growing

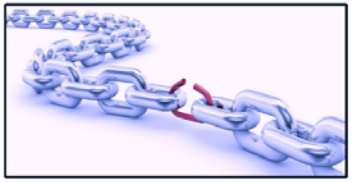
- More automation NextGen & SESAR.
- Increasing connectivity & access points - SWIM
- Unprotected data communication standards
- COTS components for interoperability with public exploits

- Flight operational and planning data.
- Weather and traffic surveillance data.
- Position, navigation and timing data.
- Controller-pilot automated messages and voice communication.
- Aircraft status data.
- Airport surface area communication.
- Security relevant data

How to face the Cyber Risk

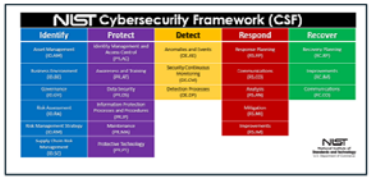
Cyber Risk = Likelihood x Impact. This means that the total amount of risk exposure is the probability of an unfortunate event occurring, multiplied by the potential impact or damage incurred by the event.

Cyber threats involve the possibility of a malicious attempt to damage or disrupt a computer network or system to access files and infiltrate or steal data..



Vulnerabilities & Control Deficiencies are associated with the quality or state of being exposed to the possibility of being attacked or compromised.

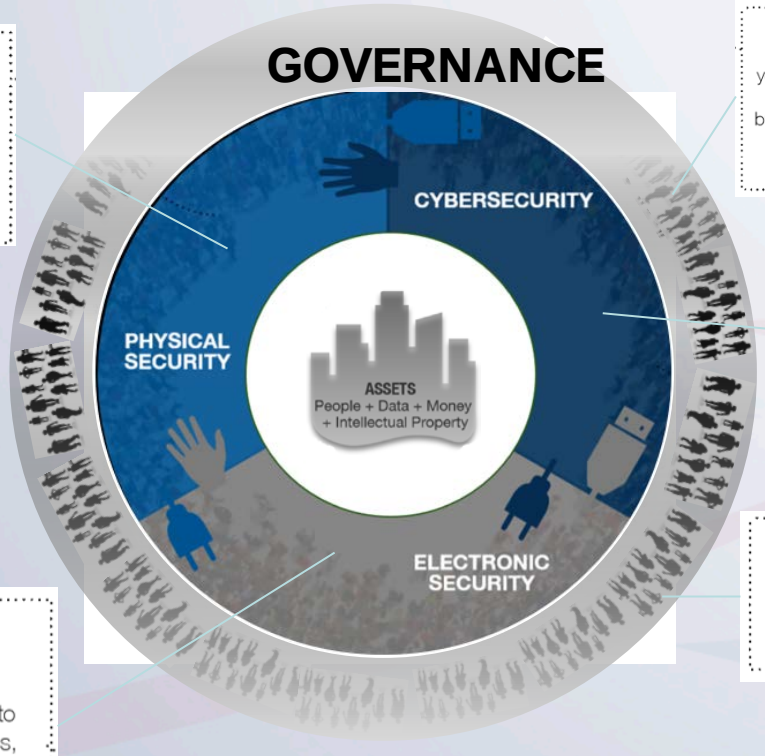
Digital Assets and Information Resources, in essence, is anything that exists in a binary format and comes with the right to use.



A controls framework is a data structure that organizes and categorizes an organization's internal **controls**, which are practices and procedures established to create business value and minimize risk.

Security Controls are safeguards or countermeasures to avoid, detect, counteract, or minimize security risks to physical property, information, computer systems, or other assets..

Integrated security model



PHYSICAL SECURITY
Buildings, Guards, Gates and other physical measures in place to secure your assets.
The Physical Firewall

HUMANS
The lifeblood in and around your organization that supports the success of your mission, but also the first line of defense from any attack:
The Human Firewall.

CYBERSECURITY
The systems you have in place to protect your electronic data and operational systems
The Network Firewall.

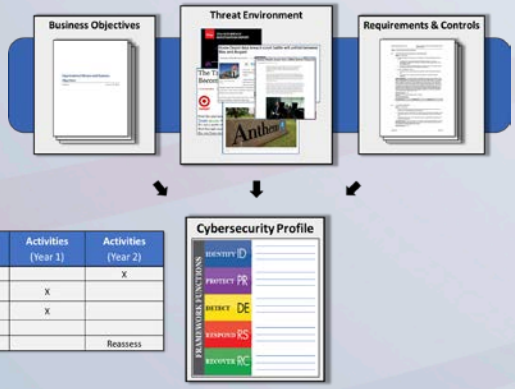
GOVERNANCE
The policies and rules set in place which support ongoing excellent security processes that keep your assets protected.

ELECTRONIC SECURITY
Devices ranging from surveillance cameras to access control badges, biometric scanners, or facial recognition systems.

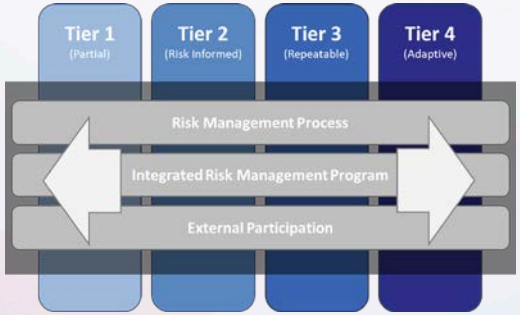
NIST Cybersecurity Framework

Function	Category	ID
Identify	Asset Management	ID.AM
	Business Environment	ID.BE
	Governance	ID.GV
	Risk Assessment	ID.RA
	Risk Management Strategy	ID.RM
	Supply Chain Risk Management	ID.SC
Protect	Identity Management & Access Control	PR.AC
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Information Protection Processes & Procedures	PR.IP
	Maintenance	PR.MA
	Protective Technology	PR.PT
Detect	Anomalies and Events	DE.AE
	Security Continuous Monitoring	DE.CM
	Detection Processes	DE.DP
Respond	Response Planning	RS.RP
	Communications	RS.CO
	Analysis	RS.AN
	Mitigation	RS.MI
	Improvements	RS.IM
Recover	Recovery Planning	RC.RP
	Improvements	RC.IM
	Communications	RC.CO

Subcategory	Informative References
ID.BE-1: The organization's role in the supply chain is identified and communicated	**COBIT 5** APO08.04, APO08.05, APO10.03, APO10.04, APO10.05 **ISO/IEC 27001:2013** A.15.1.3, A.15.2.1, A.15.2.2 **NIST SP 800-53 Rev. 4** CP-2, SA-12
ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated	**COBIT 5** APO02.06, APO03.01 **NIST SP 800-53 Rev. 4** PM-8
ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated	**COBIT 5** APO02.01, APO02.06, APO03.01 **ISA 62443-2-1:2009** 4.2.2.1, 4.2.3.6 **NIST SP 800-53 Rev. 4** PM-11, SA-14
ID.BE-4: Dependencies and critical functions for delivery of critical services are established	**ISO/IEC 27001:2013** A.11.2.2, A.11.2.3, A.12.1.3 **NIST SP 800-53 Rev. 4** CP-8, PE-9, PE-11, PM-8, SA-14
ID.BE-5: Resilience requirements to support delivery of critical services are established	**COBIT 5** DSS04.02 **ISO/IEC 27001:2013** A.11.1.4, A.17.1.1, A.17.1.2, A.17.2.1 **NIST SP 800-53 Rev. 4** CP-2, CP-11, SA-14



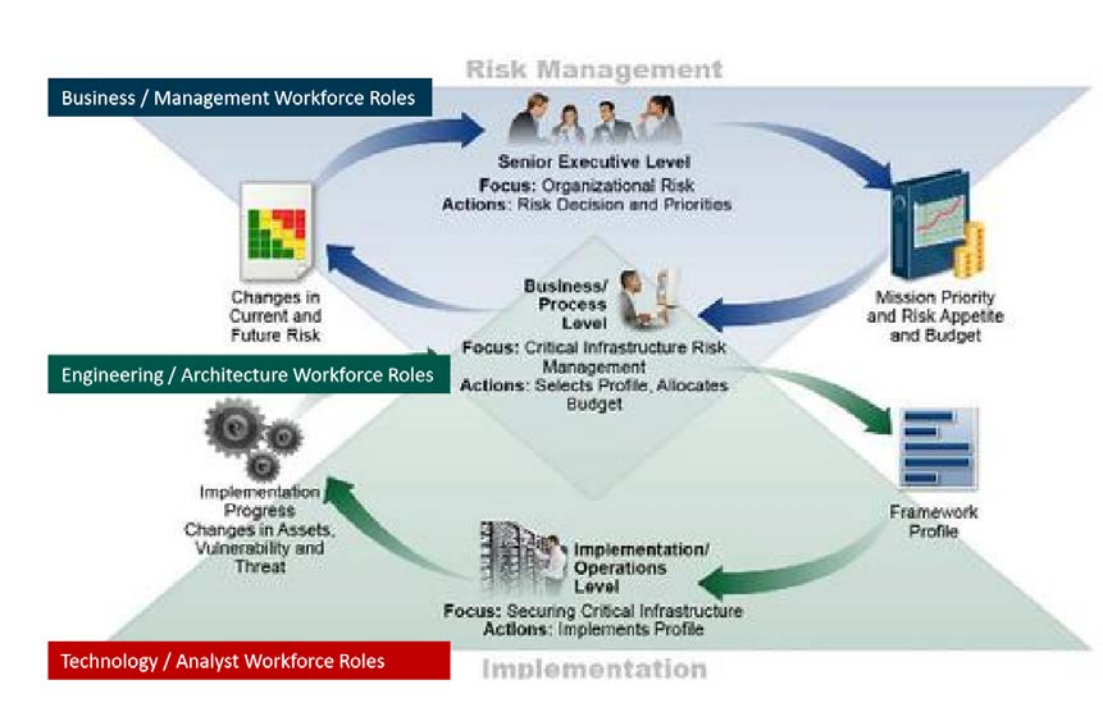
Subcategory	Priority	Gaps	Budget	Activities (Year 1)	Activities (Year 2)
1	Moderate	Small	$$$		X
2	High	Large	$$	X	
3	Moderate	Medium	$	X	
...	...	...	...		
98	Moderate	None	$$		Reassess



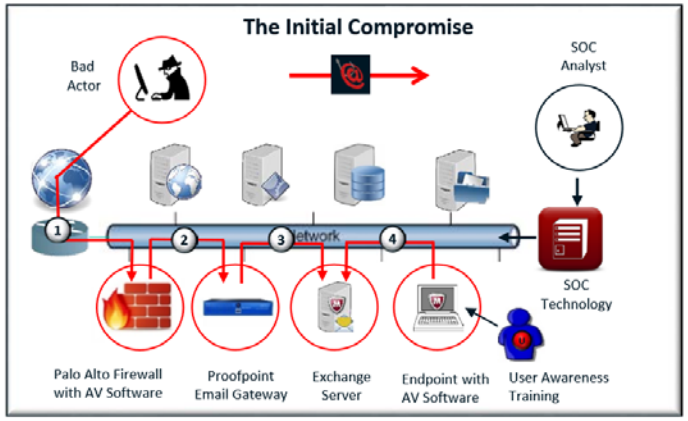
Security Plan four primary deliverables

System Security Plan (SSP)	1. The SSP should adequately describe your organization's security requirements.	The System Security Plan 
Cybersecurity Risk Assessment	2. Evaluate the security controls documented in the SSP to determine the extent to which the controls are implemented, operating as intended, and producing desired outcome.	 Example Risk Assessment Worksheets
Plan of Action & Milestones (POA&M)	3. A specific, measurable, achievable, relevant, and time-bound plan to mitigate security gaps identified in the Risk Assessment.	The POA&M 
Executive Scorecard	4. Provides a review and action plan that includes the target state profile, the current state profile, gap analysis, POA&M and overall cybersecurity maturity.	Executive Scorecard 

Involving all organization levels and all business process

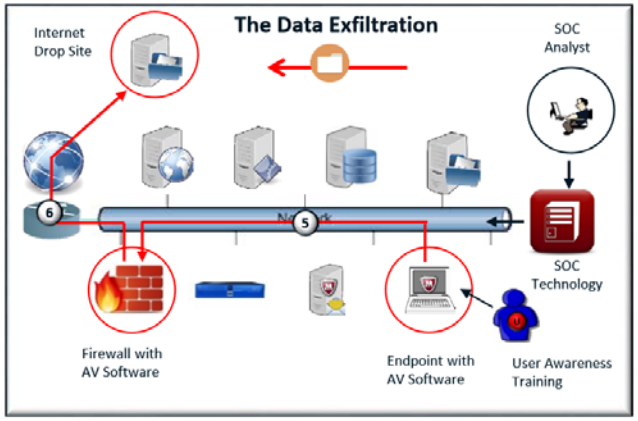


A malware Attack



What is Malware?

General term for malicious software that includes viruses, worms, trojans and spyware. Malware is a set of instructions that run on your computer and make your system do something that an attacker wants it to do.



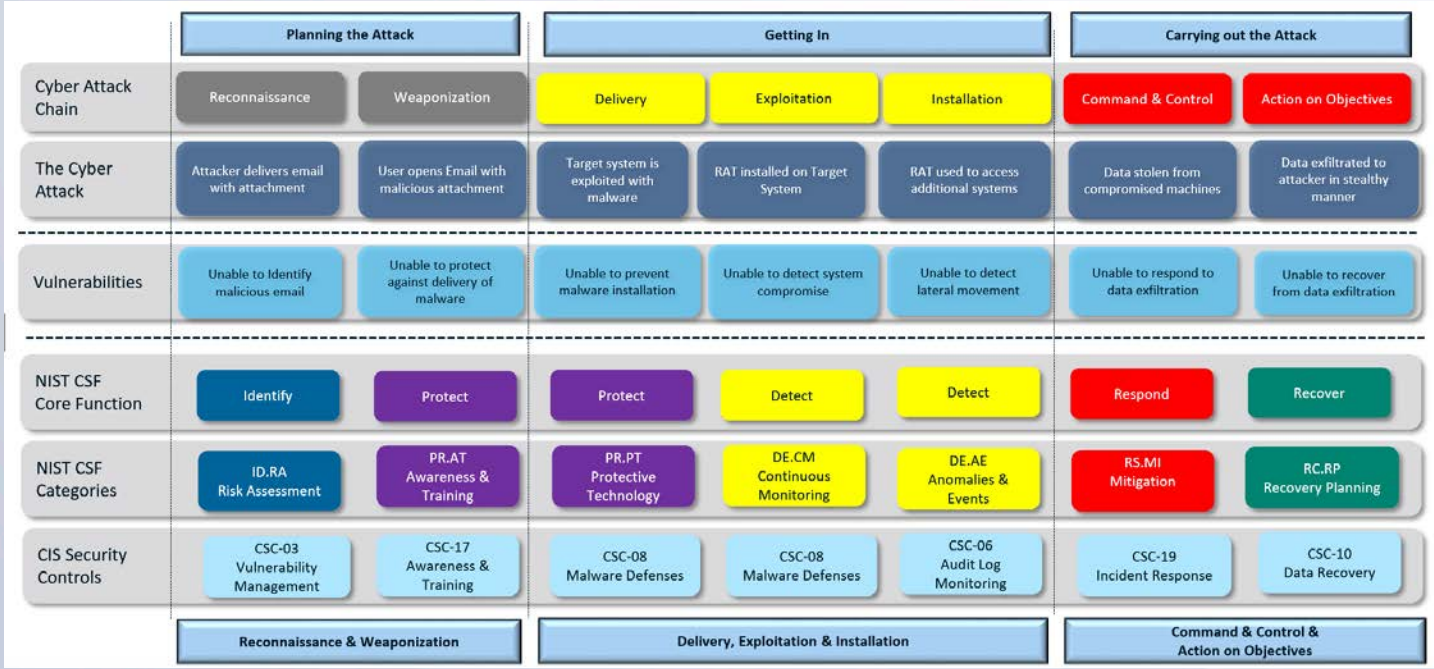
Malware Attack Controls

Before the Attack
- Scan network and systems for vulnerabilities
- Patch software and firmware to the latest version
- Whitelist applications to define legitimate software
- Implement malware detection for inbound / outbound channels

During the Attack
- Control access to assets based on need to know
- Use available tools on malware analysis and mitigation

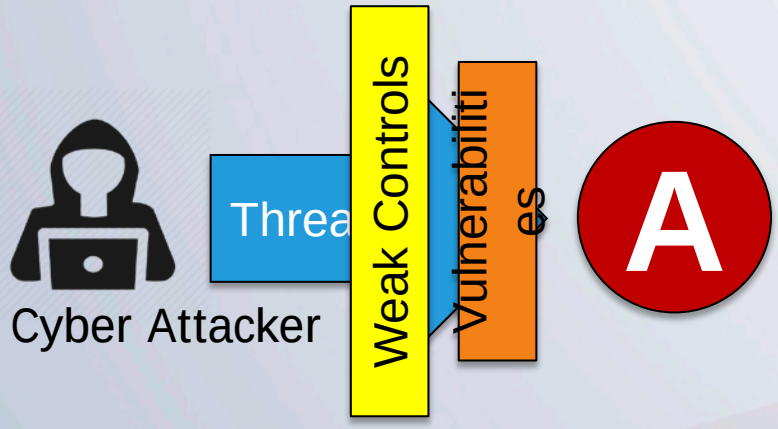
After the Attack
- Analyze malware to determine impact
- Establish incident management for efficient response capabilities

Mitigating Malware Attacks



What Problem are we trying to Solve?

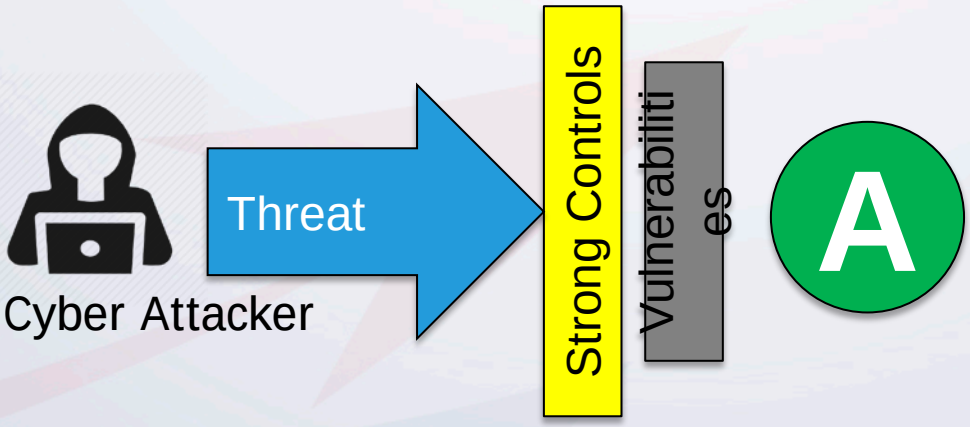
- Unmanaged Assets: Weak security controls



Our Unmanaged Assets are at a High Risk

This means a higher opportunity or higher likelihood of a compromise or unintended outcome

- Managed Assets: Strong security controls



Our Managed Assets are at a Lower Risk

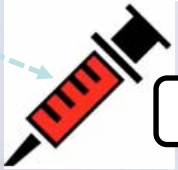
This means a lower opportunity or lower likelihood of a compromise or unintended outcome

Steps to fix a Cybersecurity Breach

IDENTIFY

PROTECT

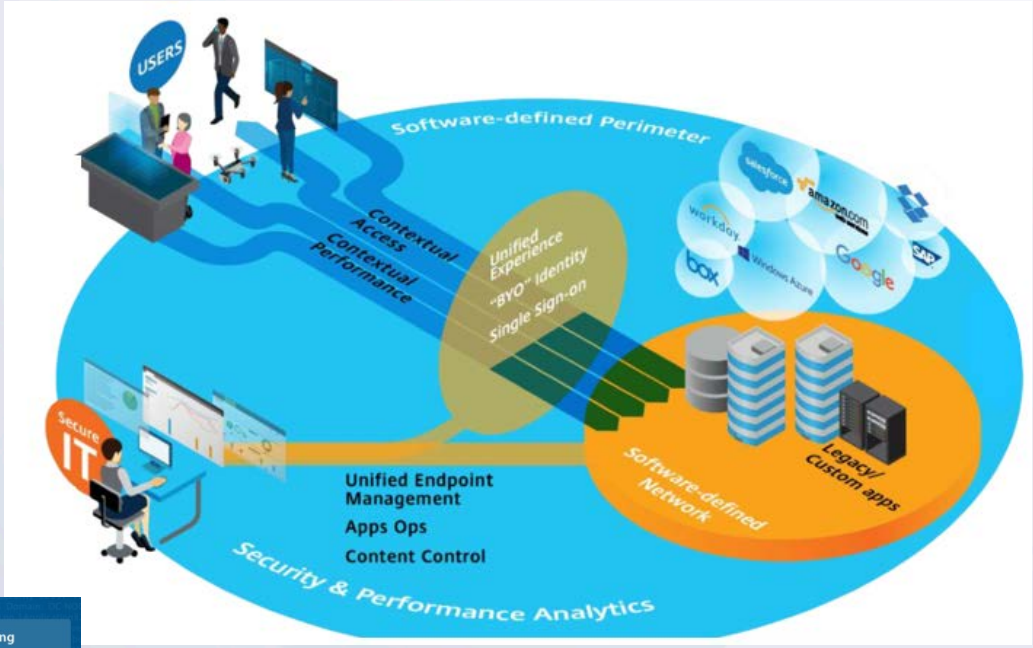
DETECT

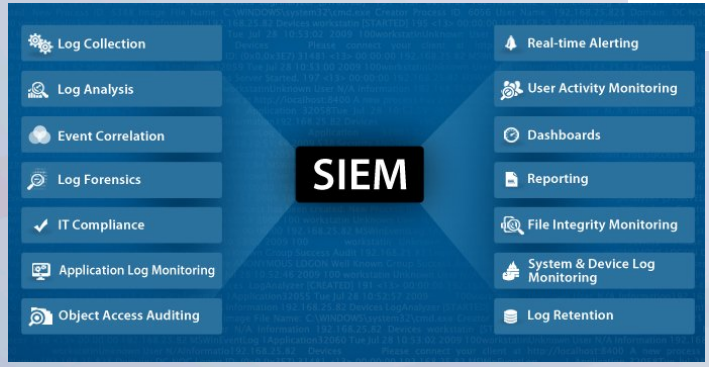


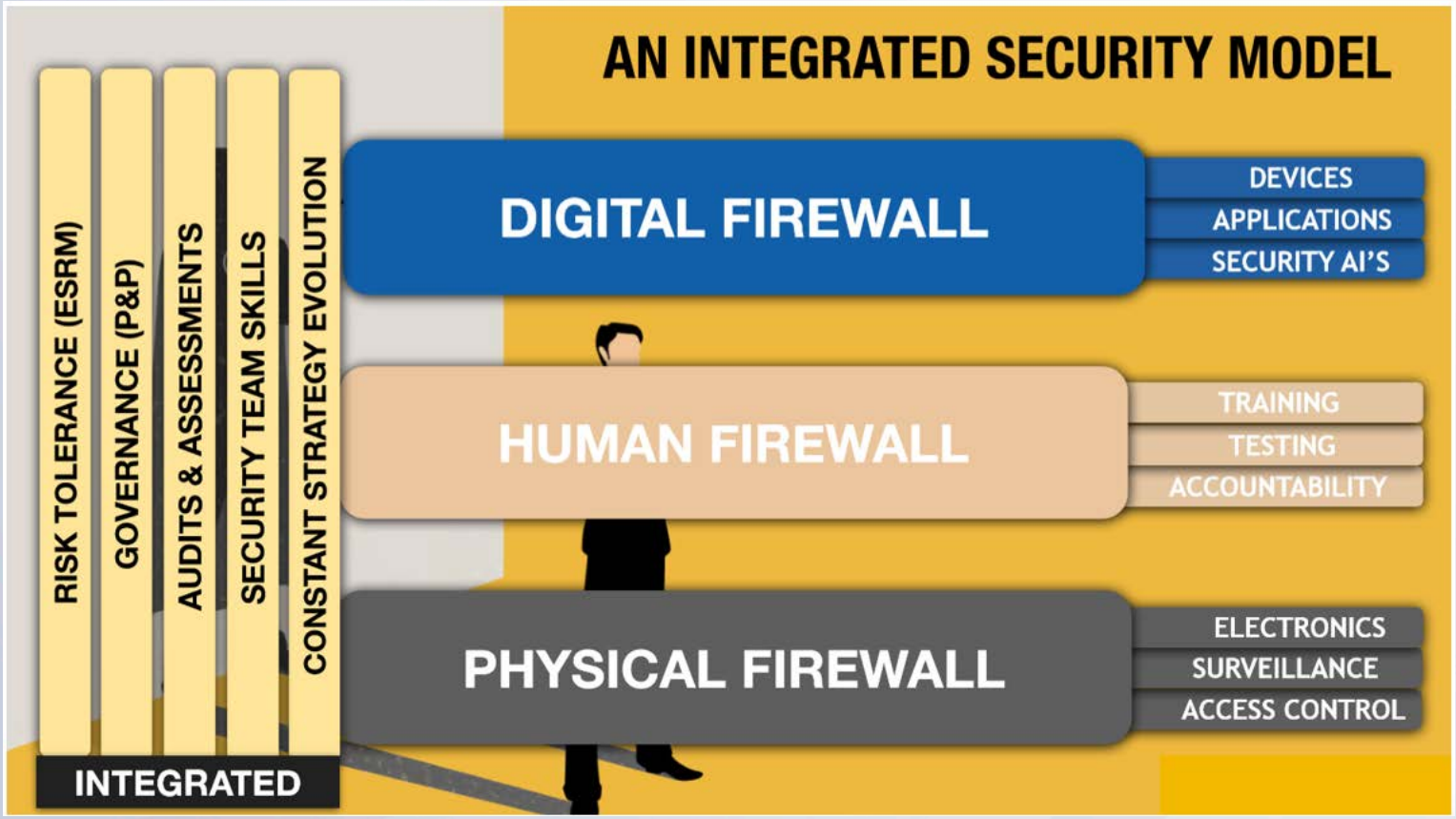
RESPOND

RECOVER

Security Information and Event Management (SIEM)






AN INTEGRATED SECURITY MODEL
RISK TOLERANCE (ESRM)
GOVERNANCE (P&P)
AUDITS & ASSESSMENTS
SECURITY TEAM SKILLS
CONSTANT STRATEGY EVOLUTION
INTEGRATED
DIGITAL FIREWALL
DEVICES
APPLICATIONS
SECURITY AI'S
HUMAN FIREWALL
TRAINING
TESTING
ACCOUNTABILITY
PHYSICAL FIREWALL
ELECTRONICS
SURVEILLANCE
ACCESS CONTROL

canso

civil air navigation services organisation

Transforming Global ATM Performance