Session 8- Building Cyber Resilience: Regulations Perspective

Ms. Nada Khater

Eng. Nada Khater is the division head of e-government strategies at the Ministry of digital economy & entrepreneurship of Jordan.

She is also Aided in the developing Jordan's Government General Policy for information technology, telecommunications, digital transformation & Postal Sectors in 2018.

In addition, eng. Nada participated in the developing and issuance of National CyberSecurity Strategy 2018-2023, CyberSecurity policies framework 2019, and recently Jordan's CyberSecurity Law in 2019

Nada Khater

Division Head of E-Government Strategies
Policies and Strategies Directorate
Ministry of Digital Economy and Entrepreneurship
Nada.khater@modee.gov.jo
Nadakhater83@gmail.com

Introduction

وزارة الاقتصاد الرقمي والريادة

- In May 2019, a Ministry for Digital Economy and Entrepreneurship (MoDEE) has been established

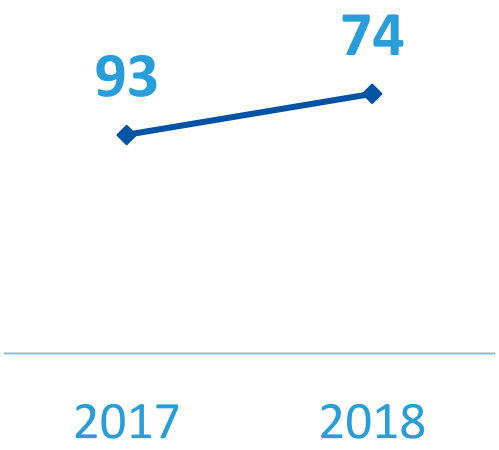
- MoDEE is the legal successor of the Ministry of Information and Communication Technology (MoICT).

Content

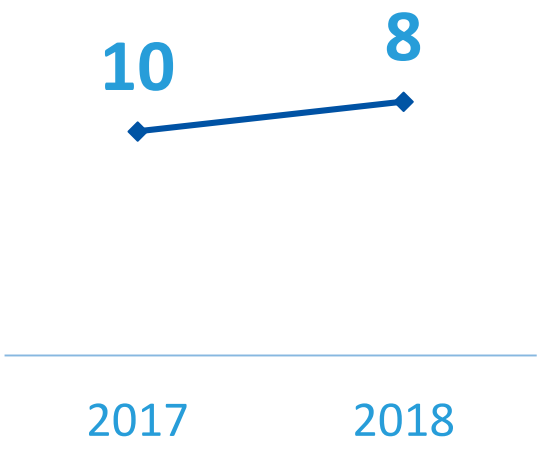
- National Cyber Security Strategy 2018-2023
- Cyber Security Policies Framework 2019
- Jordan’s Cyber Security Law No. 16 for the year 2019

Global Cyber Security index (GCI)

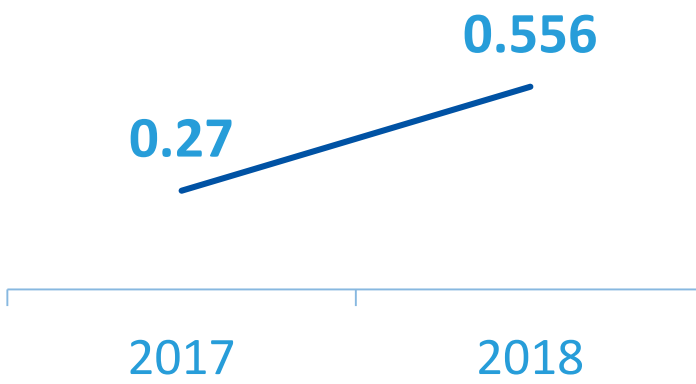
Global rank of Jordan



Regional rank of Jordan



Jordan Score



Background

- 2012: The Government of Jordan published the National Information Assurance and Cyber Security Strategy (NIACSS).

- 2015: National Cyber Security Program (NCP) has been established to deliver the strategic objectives.

2012 Strategy Achievements

Completed a critical network risk assessment program

Delivered a cyber training program

Created specific national Computer Emergency Response Teams (CERTs)

Established a Public Key Infrastructure (PKI)

Started establishing an international information security co-operation program

Established the foundations for a National Cyber Academy

National Cyber Security Strategy 2018-2023

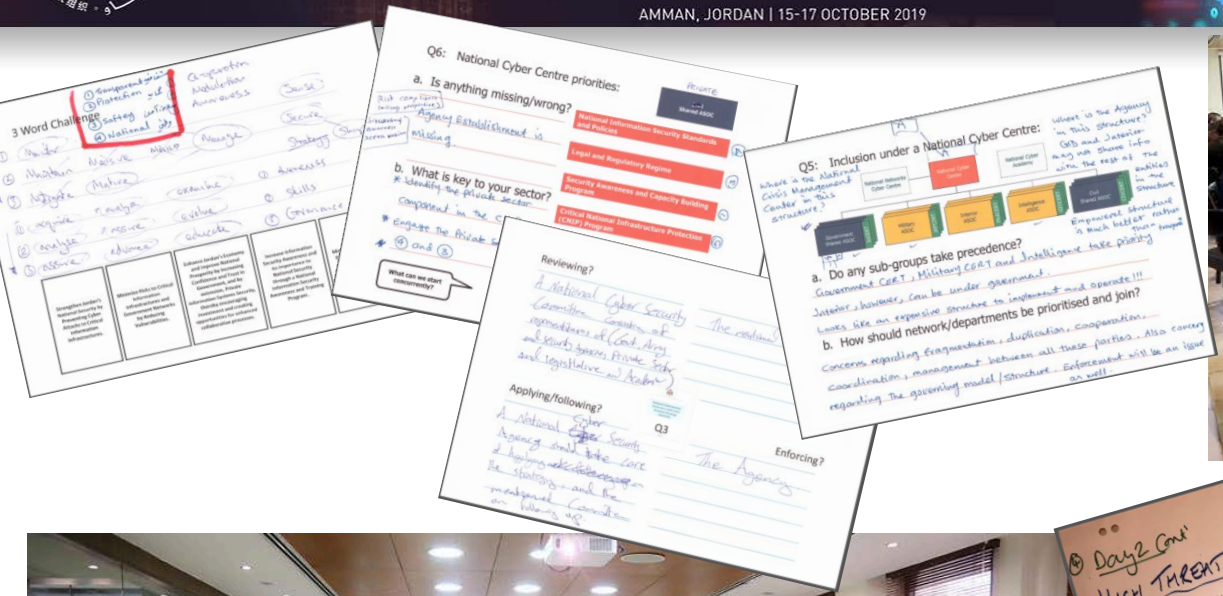
ICAO MID

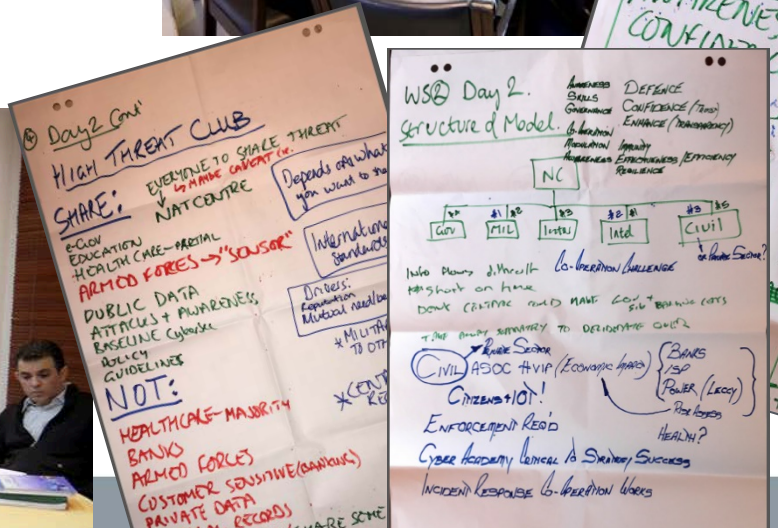
CYBER SECURITY AND RESILIENCE SYMPOSIUM

TOWARDS A RESILIENT AVIATION CYBERSPACE

AMMAN, JORDAN | 15-17 OCTOBER 2019

ICAO 2019
75 YEARS OF CONNECTING THE WORLD





National Cyber Security Strategy 2018-2023

- Vision:
  - confident and secure in the digital world and resilient to cyber threat.

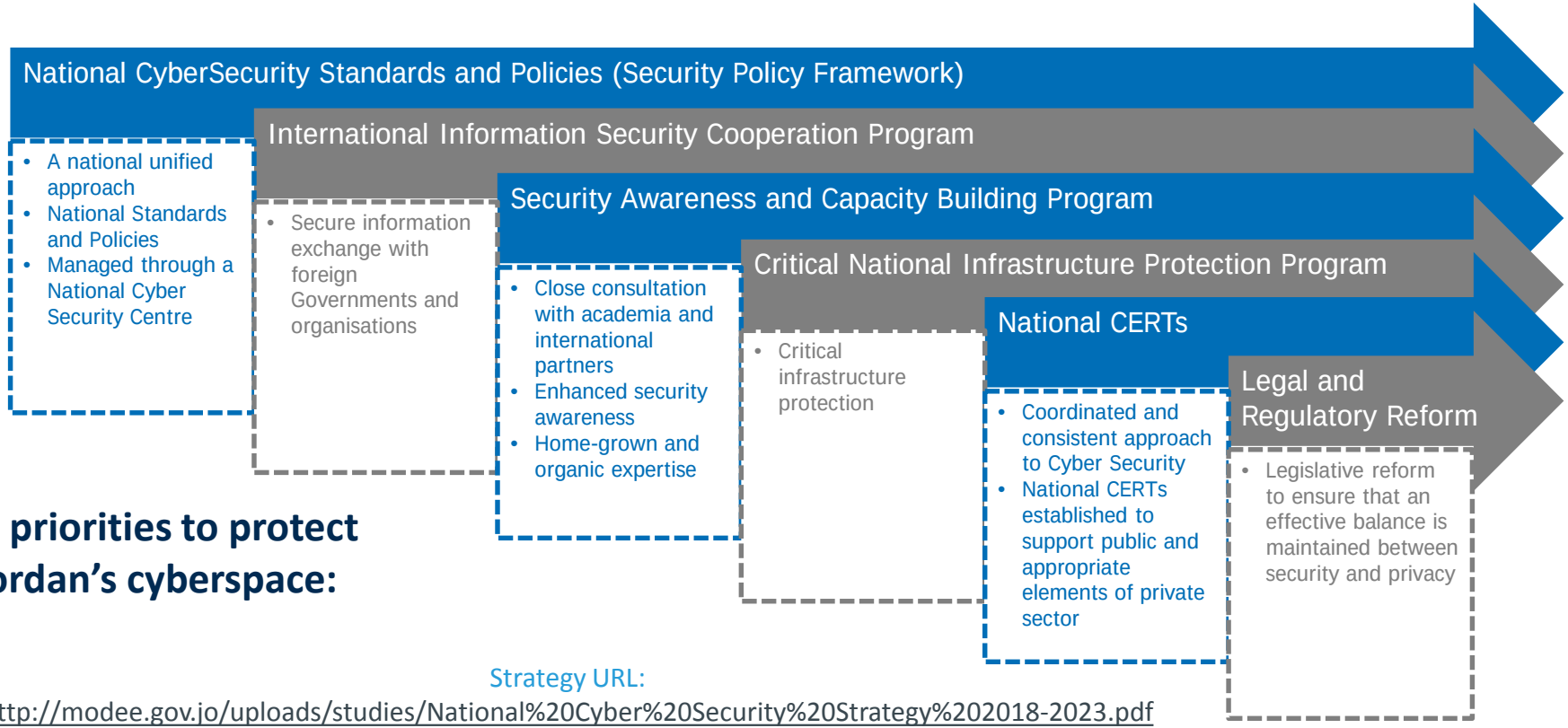
Four strategic objectives :

- Publishing policies, and procedures
- Establishing an appropriate governance / organisational structure
- Establish a cyber security awareness and capacity building program

- Evolving capabilities
- Understanding behavior of adversaries
- Continuity of detecting events
- Classification of events

- Partnering
- Enacting the legislation and regulation needed
- Sustainable Means
- communication channels.

- Processes, Capabilities and Mitigation
- containing the impacts.
- Using root cause analysis



Six priorities to protect Jordan's cyberspace:

Strategy URL:
http://modee.gov.jo/uploads/studies/National%20Cyber%20Security%20Strategy%202018-2023.pdf

Cyber Security Policies Framework 2019

Cyber Security Policy Framework (CSPF)

DESCRIBED SECURITY AREAS	SUPPORTING POLICIES				
Core Area 1 Governance, Risk Management & Compliance	**1.A Roles, Accountability & Responsibilities** Who does what, and who is responsible to whom	**1.B Risk Management** How to assess, score, and manage Risk	**1.C Audit & Assurance** Methods to conduct audit and gain assurance	**1.D International Compliance** Standards required for international collaboration	
Core Area 2 Protective Marking, Resourcing & Asset Control	**2.A Protective Marking System** Classification system in use, including special handling and the criteria for applying	**2.B Protection & Disclosure** Control of, marking, and disclosure of assets and information	**2.C Resource Management** Supplier assurance and relations		
Core Area 3 Personnel Security	**3.A Personnel Security Standards** Procedures for applying, checking, renewing, reviewing, and withdrawal	**3.B Security Clearance** Levels and duration of security clearance			
Core Area 4 Information Security & Assurance	**4.A Information Security** Protection of live, transmitted, and data at rest, including online and offline storage and acceptable use	**4.B Information Assurance** Gaining formal accreditation and meeting audit requirements	**4.C Configuration Management** Network configuration and joining	**4.D Portable Devices** Use of storage, transmitting, and recording devices	**4.E Protective Monitoring** Policy enforcement, compromise detection
Core Area 5 Physical Security	**5.A Defence in Depth** Establishing secure perimeters and layers of security	**5.B Containers & Storage** Secure furniture, rooms, and storage requirements	**5.C Physical Access** Access controls and visitor control		
Core Area 6 Business Continuity	**6.A Change Management** Planning, releases, changing and roll-back	**6.B Incident Response** Analysing, escalating, and responding to incidents	**6.C Continual Improvement** Lessons, reviews, and continual improvement		

Cyber Security Policy Framework (CSPF)

CSPD URL: http://modee.gov.jo/content/national-cyber-security-policies-619

National Cyber Security Law No. 16- 2019

National Cyber Security Law No. 16- 2019

- **The Journey of Cybersecurity law:**
  - April 2019, the government formed a committee to prepare a draft of Cybersecurity law
  - End of May, 2019, The committee submitted its draft to the cabinet
  - July 2019, The law passed to the parliament for their approval
  - The Royal Decree was issued approving the law in 16h of September 2019

Governance

Prime Minister

Provides empowerment/oversees

Cyber Security Council

- Virtual Organisation with representation from Public and Private sector
- Sets strategic direction and monitors progress of the strategy implementation

National Cyber Security Centre

- **Strategic role for:**
  - Management of National Cyber security Program
  - Relationships & Partnerships
  - Skills Development & Cyber Awareness
  - Strategy Development
- **Operational role for:**
  - Threat Intelligence & Situational Awareness
  - Cyber Risk & Compliance
  - Incident Response & Management


Cyber Security Council
Government
Defense & Security
Private sector
Financial Sector
Chaired by a Senior Government Official

National Cybersecurity Centre

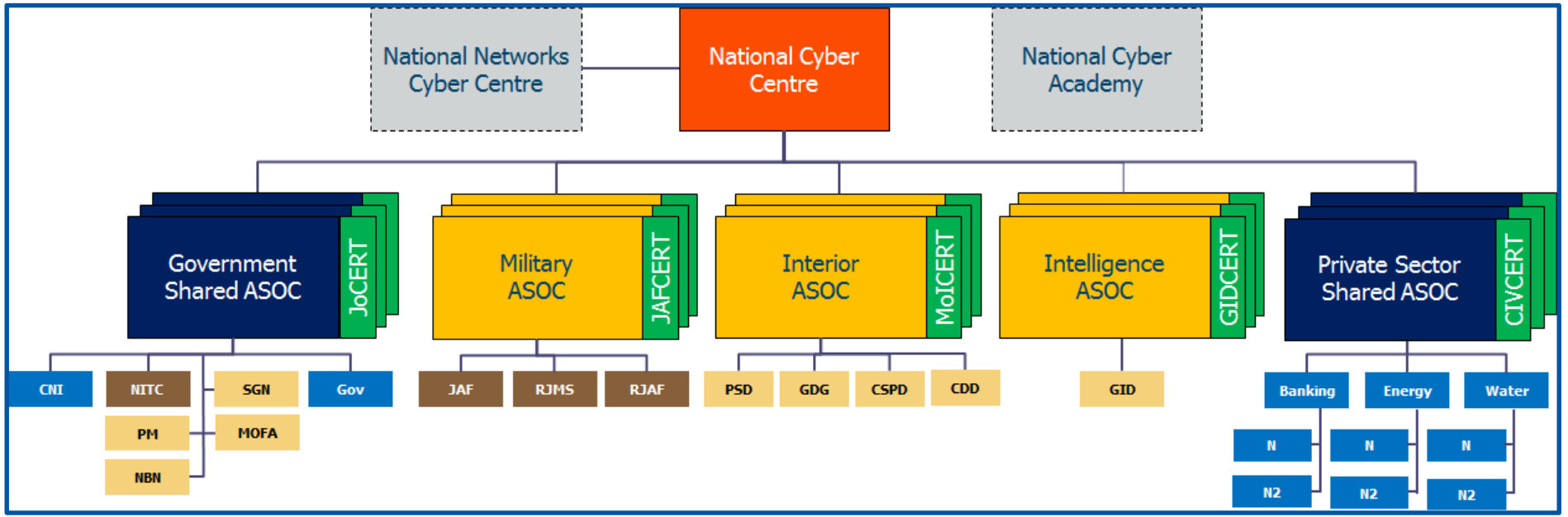
Strategic role

- Management of National Cyber security Program
- Relationships & Partnerships
- Skills Development
- Cyber Awareness
- Strategy Development

Operational role

- Threat Intelligence & Situational Awareness
- Cyber Risk & Compliance
- Incident Response & Management

Suggested relations between CERTs



References

- All the cyber issues (legislation, strategies, policies, public news) can be found on the Ministry website (www.modee.gov.jo).

- Here are some specific links that have been used in the presentation:
  - http://modee.gov.jo/content/legislation-589
  - http://moict.gov.jo/content/national-cyber-security-policies-619
  - http://moict.gov.jo/uploads/studies/National%20Cyber%20Security%20Strategy%202018-2023.pdf
  - http://moict.gov.jo/uploads/ICTP_Policy_2018.pdf


CYBER SECURITY AND RESILIENCE SYMPOSIUM
TOWARDS A RESILIENT AVIATION CYBERSPACE
AMMAN, JORDAN | 15-17 OCTOBER 2019
ICAO
Thank You

Ms. Hana Guyaux Pecháčková

Ms. Hana Guyaux Pecháčková holds a master degree in law and jurisprudence (2000) from the Masaryk University Brno, Czech Republic.

Since 2000 she worked for several international law firms where she focused on competition, telecommunication and electronic communication, e-commence, intellectual property rights and IT & new technologies.

Ms Guyaux Pecháčková has joined the European Commission in July 2005 as a legal officer at Directorate-General Justice, Freedom and Security. Ms Guyaux Pecháčková worked in the field of data protection and privacy, dealing with data protection and privacy related issues in new technologies.

In October 2011, Ms Guyaux Pecháčková joined the European Commission's Directorate-General for Mobility and Transport/ (Aviation) Security unit. She is the Secretary of the Aviation Security Committee and Stakeholders Advisory Group on Aviation Security and is responsible for cyber security policy and coordination.

Hana Guyaux Pecháčková

European Commission

Directorate General for Mobility and Transport

Security

Building Cyber Resilience: Regulations Perspective

- No borders for cyber attacks
- BUT: response capacity differs across borders
  - Need for more robust and effective structures
  - Nobody wants to be the weakest link
  - Need to find common solutions
- Are good practices good enough at this stage?

Building Cyber Resilience: Regulations Perspective

- EU policy response
  - 2008 Critical European Infrastructure Protection Directive
  - 2013 EU Cybersecurity Strategy
  - 2015 Digital Single Market Strategy,
  - 2016 PPP on Cybersecurity, NIS Directive, EASA Roadmap
  - 2017 European Strategic Coordination Platform
  - 2019 Cybersecurity Act, AVSEC Implementing regulation “Preventive measures“, ECCSA, ESCP European Cybersecurity strategy

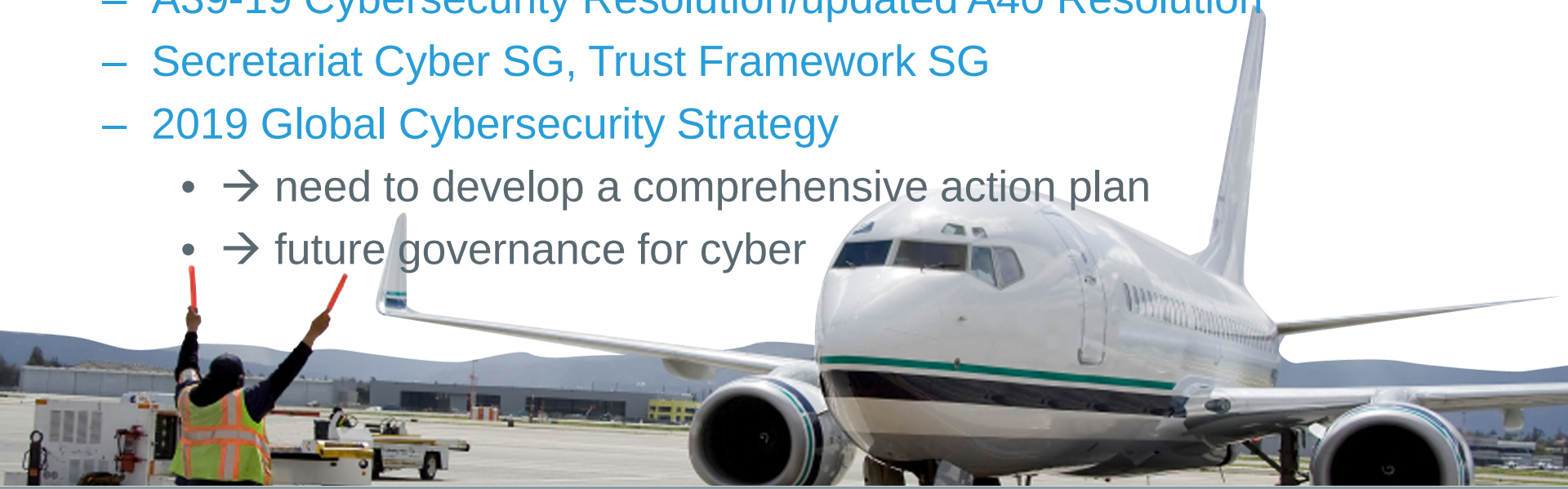
Building Cyber Resilience: Regulations Perspective

- Not only regulating, but supporting stakeholders in implementation
  - Focus on human element
  - Cultivating cybersecurity culture
- Work across domains, countries & regions to face global challenge

Building Cyber Resilience: Regulations Perspective

Global level / ICAO major milestones

- A39-19 Cybersecurity Resolution/updated A40 Resolution
- Secretariat Cyber SG, Trust Framework SG
- 2019 Global Cybersecurity Strategy
  - → need to develop a comprehensive action plan
  - → future governance for cyber



Building Cyber Resilience: Regulations Perspective

Way towards resiliency and stronger system:

→All relevant actors must work together, break silos:

- internally within organisations
- with partners in the aviation sector and beyond
- with partners in other countries

Also in Cyber: No Country Left Behind


CYBER SECURITY AND RESILIENCE SYMPOSIUM
TOWARDS A RESILIENT AVIATION CYBERSPACE
AMMAN, JORDAN | 15-17 OCTOBER 2019
ICAO
Thank You

Mr. Biju Hameed

Mr. Biju Hameed is a seasoned cybersecurity professional & international speaker with over eighteen years of extensive experience in the areas of cybersecurity management & operations with in depth knowledge on technology & business domains. He currently heads the Cybersecurity & Resilience practice at a Dubai Airports.

He is currently a sitting advisory board member for the Gartner GCC Security & Risk Management Summit (since 2015) and Palo Alto's EMEA Executive Advisory Board. He has also been awarded the (ISC2) Committee Choice Awards (MESA) 2018 and has been a recipient of the MESA CISO100 Information Security Executive Award for the past 3 years.

Biju Hameed CISSP, CISM, CRISC, CISA, CCSP
HEAD OF CYBERSECURITY & RESILIENCE – DUBAI AIRPORTS

THE CHANGING LANDSCAPE OF THREATS AGAINST CRITICAL INFRASTRUCTURE ENVIRONMENTS

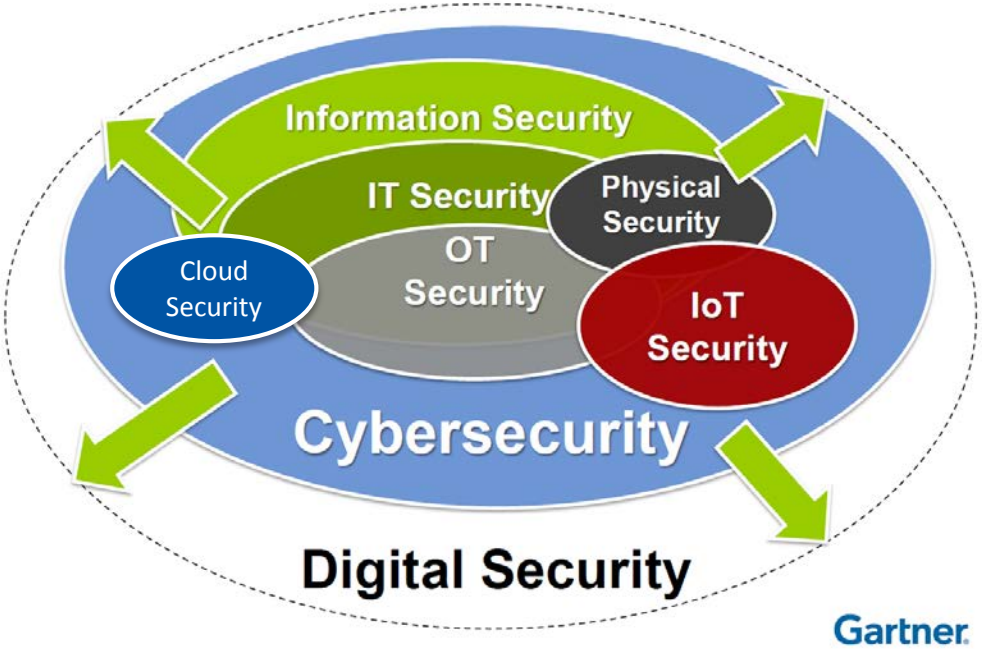
Disclaimer:

The views and the points presented here are the personal & professional views of the speaker and do not necessarily reflect the views of Dubai Airports

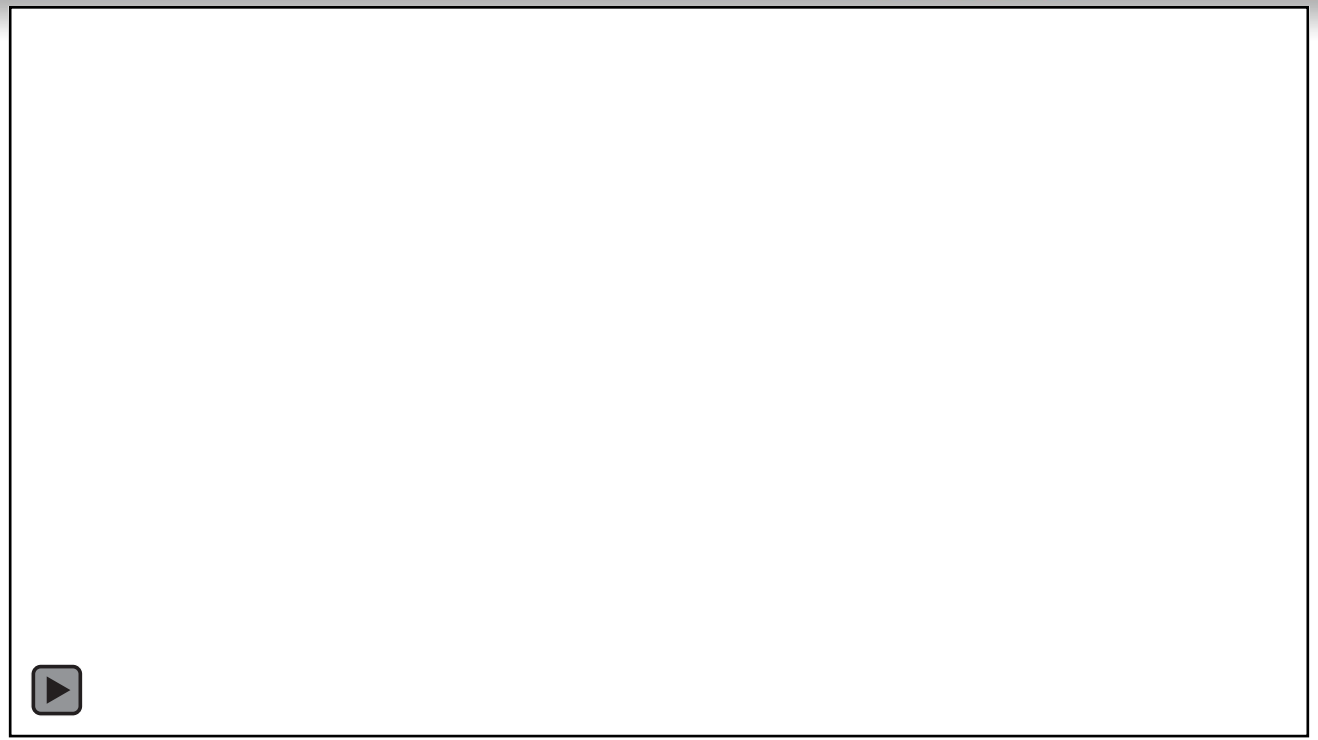
"Some organizations will be a target regardless of what they do, but most become a target because of what they do"

Verizon DBIR

Cyber-Physical Landscape

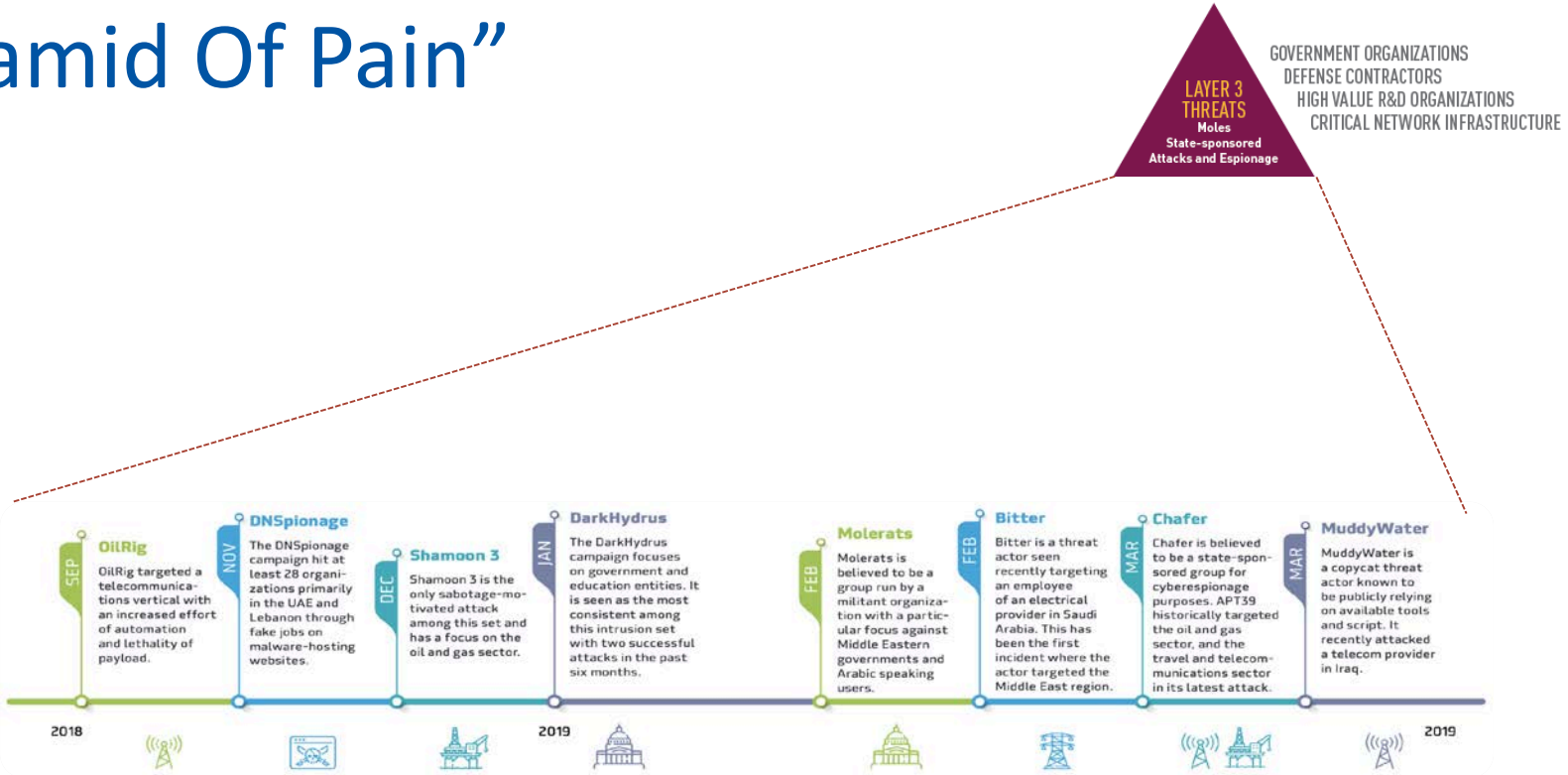


Perspective: Typical Airport Environment



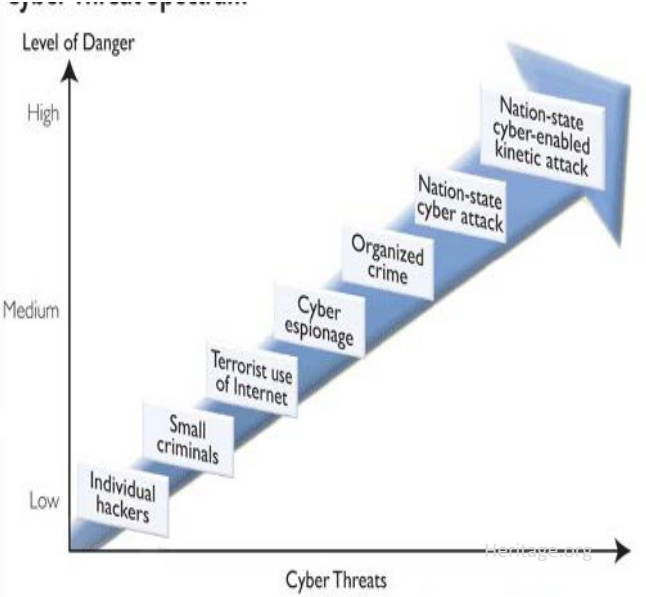
COINCIDENCE OR ORCHESTRATED ATTACK?

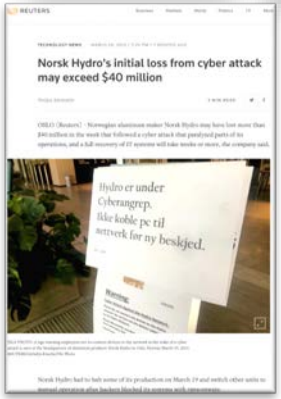
"Pyramid Of Pain"



Source: Darkmatter Report July 2019

Broad-spectrum Impacts

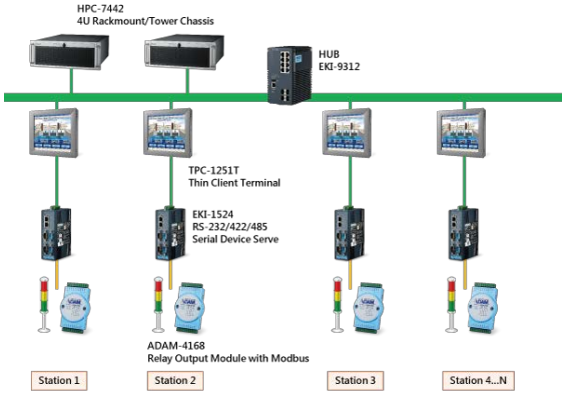




https://www.google.com/url?sa=i&source=images&cd=&ved=2ahUKEwj--4-hgprlAhWE26QKHUvrDvMQjRx6BAgBEAQ&url=https%3A%2F%2Fwww.bleepingcomputer.com%2Fnews%2Fsecurity%2Fnew-greyenergy-malware-targets-ics-tied-with-blackenergy-and-telebots%2F&psig=AOvVaw0HGZiVvcFalniG5K3lfnJr&ust=1571082944908182

Current state of our OT Infrastructures

- **40%** of industrial sites have at least one direct connection to the internet
  (The “air-gap” is still a myth)
- **84%** of sites have at least one remotely accessible device
  (Excessive accessibility)
- **53%** of industrial sites have outdated Windows systems like XP
  (Broken Windows)
- **69%** have plain-text passwords traversing the network
  (Hiding in plain sight)
- **57%** of sites are still not running malware protections that update signatures automatically (Anti-anti-virus)



Source: CYBERX Report 2019

The Underlying (& overlooked) Risks!

- Disproportionate Understanding (AVSEC vs. CYBERSEC)
- Sector Growth with increasing Availability & Inter-connectivity needs
- Fast adaptation of Social-Mobility-Analytics –Cloud (SMAC)
- Proliferation of NextGen Airport Solutions, e-Enabled Aircrafts & the Hyper-Connected Passenger
- Not enough visibility into Supply Chain Security
- Overlooking the OT (SCADA/ICS) space
- Ignoring basic cybersecurity hygiene (segmentation, patching, upgrading…)!

As Organizations, we….

SHOULD FOCUS ON FUNDAMENTALS & GO BACK TO THE BASICS!

NEED TO MOVE TO RISK-CENTRIC & DATA-DRIVEN DECISION MAKING

MUST UNDERSTAND THAT 80 / 20 PRINCIPLE IS STILL VERY MUCH APPLICABLE

NEED TO WORK TOWARDS INTEGRATING "IT" & "OT" CYBER SECURITY AND RESILIENCE INTO CYBER-PROGRAMME

MORE SECURITY TOOLS DOES NOT MAKE YOU MORE SECURE, BETTER MANAGEMENT DOES!

Bringing in True Cyber-Resilience

- Ability to Adapt to Changing Conditions
- Withstanding Disruptions
- Ensuring Rapid Recovery
- Adopting Cyber Insurance for key sectors

“It takes twenty years to build a reputation and five minutes to ruin it. If you think about that, you’ll do things differently.”

Warren Buffet


CYBER SECURITY AND RESILIENCE SYMPOSIUM
TOWARDS A RESILIENT AVIATION CYBERSPACE
AMMAN, JORDAN | 15-17 OCTOBER 2019
ICAO
Thank You

Ms. Samiha Al Busaidi

Samiha Al Busaidi is Oman Air's Manager Security Network & Compliance. She has been in the aviation industry for over 16 years out of which 9 with the Security Department. An MBA holder with double degrees Major in Economics and minor in Accounting & Finance and an ICAO-AVSEC PM.

In her years of experience with Oman Air, she is responsible for the entire network (Asia, Africa & Europe) security operations looking after the compliance to the various CAA's requirements, Security Quality Control, Training & Investigations. She is an AVSEC Auditor, Trainer and Investigator.

Samiha Al Busaidi

Manager Security Network & Compliance

Airline Initiative

- In compliance with Annex 17 & recommendations of the NCASP, Oman Air's main objective in terms of Cyber Security, is to achieve a continued safe & secure operation against the existing & emerging cyber threats.
  - creation of a strategy that will ensure the sustainability of the operation through application of security measures that will protect critical information and communication systems, including hardware and software, against cyber-attacks and interference.

Compliance Strategy

- Identify & Detect
- Develop and Implement
- Protect & Mitigate
- Evolve & Redevelop

Identify & Detect

- Identify critical information & systems
  - Access Control, Departure Control & Traffic Control Systems …etc.
- Conduct risk assessment involving all stakeholders (joint venture between regulators & industry)
- Establish the scope of work & responsibilities

Develop and Implement

- Develop protective measures based on identified risks.
  - Standards & Procedures
  - Systems that protect & deter
    - Administrative Control, Logical/virtual Controls & Physical Controls
- Promote & Raise Cyber Awareness
  - Improve cyber community
    - Collaboration, enhance cyber capability …etc.
  - Raise awareness (cyber security culture)

Manage & Mitigate

- Establish a monitoring & reporting system
  - Emerging incident monitoring systems
  - Enhance information sharing & facilitate incident reporting mechanism
- Manage Cyber Risks and take appropriate action
  - Develop response plan with appropriate CAP
    - Comply with regulatory framework
    - Mitigate & reduce impact
  - Ensure business recovery/continuity (backup/CAP)

Evolve and Redevelop

- Project flexibility and adaptation
  - Continuous identification and assessments of risk
  - Technological upgrades / advancements vs associated risks that might compromise the system
  - Proactive approach in facilitation technology without hindering innovation.

Summary

- Risk assessment regime should ensure continuous identification of emerging risk/threats .
- As a minimum, the objectives of cyber security measures should be to protect systems (critical data) against unauthorized access/use and detect such attacks on the system.
- Successful strategy against a cyber compromise (deliberate/accidental) is based on its ability to mitigate and recover ensuring business continuation with minimum impact.


CYBER SECURITY AND RESILIENCE SYMPOSIUM
TOWARDS A RESILIENT AVIATION CYBERSPACE
AMMAN, JORDAN | 15-17 OCTOBER 2019
ICAO
Thank You

Dr. Rebekah Tanti-Dougall

Dr. Rebekah Tanti-Dougall is a Senior Associate at 'Advocates, Tanti-Dougall & Associates' Law Firm based in Malta. As part of her Legal Doctorate Degree with the University of Malta

She is author of various articles on the cyber threat, including with Benedict's Maritime Bulletin, Aviation Security International and LexisNexis.

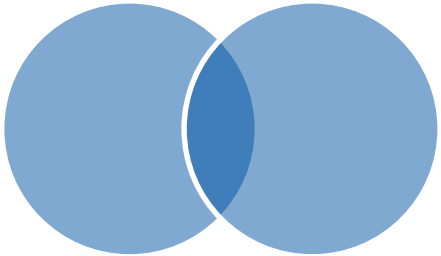
Dr. Tanti-Dougall is also legal advisor to the Bureau of Air Accidents Investigation in Malta as well as legal advisor on the legal aspects of the cyber threat in aviation to the Ministry of Home Affairs and National Security (MHAS). Dr. Tanti-Dougall represents Malta on the ICAO Secretariat Study Group on Cyber sub-group on legal matters.

Dr Rebekah Tanti-Dougall

Partner at Advocates, Tanti-Dougall & Associates Law Firm

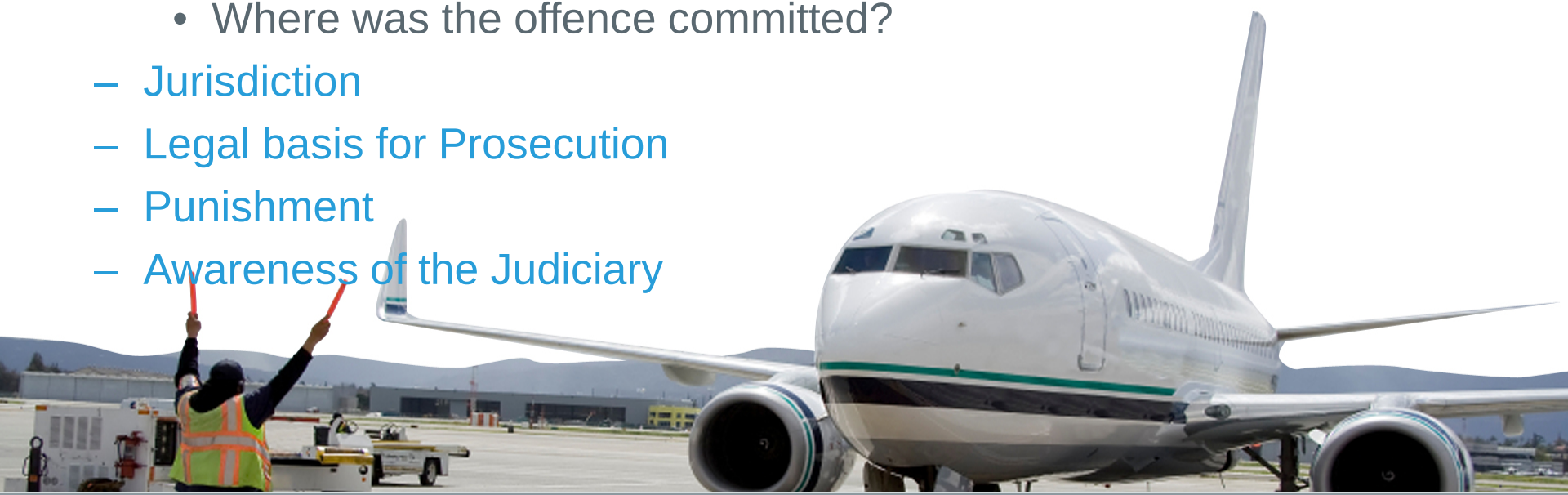
Legal Consultant on the Cyber Threat in Aviation

Cyber Security Governance and Legislative Empowerment



Legal Aspects

- Cross Border
  - Where was the offence committed?
- Jurisdiction
- Legal basis for Prosecution
- Punishment
- Awareness of the Judiciary



Legal Framework

Effective

Proactive

ICAO Cyber Security Strategy

- approporiate legislation is formulated and applied

- whether national legislation requires an update or the adoption of new national legislation to allow for the prosecution of cyber threats

Cyber Security Governance

- Awareness
- Ensure strong defences
- Quick recovery from attacks
- Table Top
- Red Teaming [Assessment]
- Cyber security culture at all levels

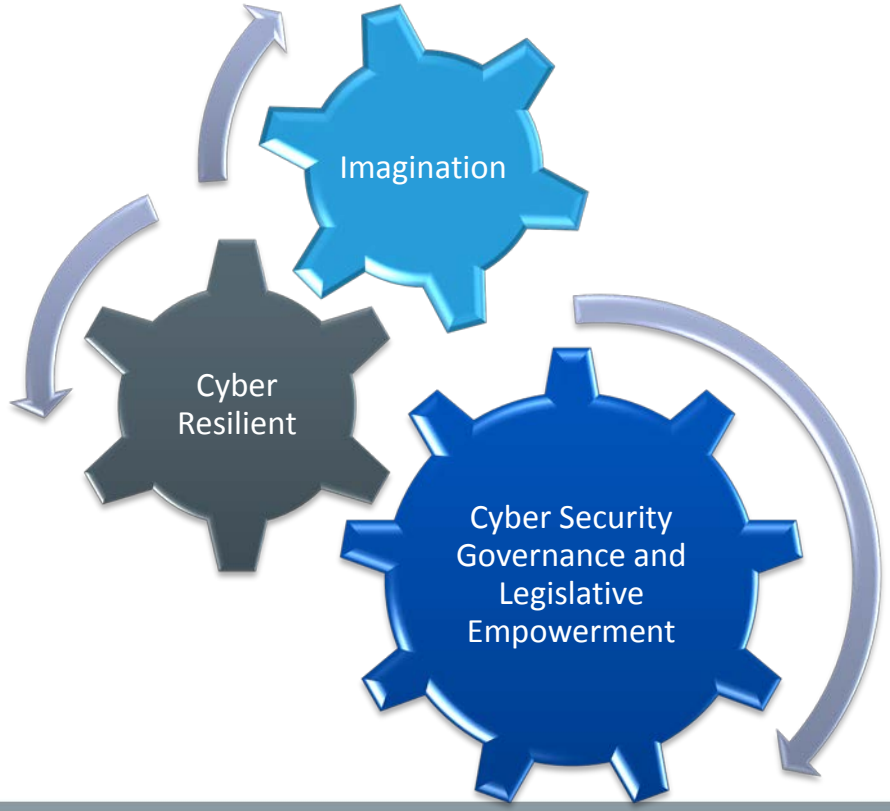
Cyber Resilient…

- Proactive vs Reactionary
- 9/11 Commission

Imagination

- Failure of Imagination…

1. Policy is not created
2. Capabilities are not developed
3. Management is not trained


Imagination
Cyber Resilient
Cyber Security Governance and Legislative Empowerment


CYBER SECURITY AND RESILIENCE SYMPOSIUM
TOWARDS A RESILIENT AVIATION CYBERSPACE
AMMAN, JORDAN | 15-17 OCTOBER 2019
ICAO
Thank You