



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

Defending Airports Against Emerging Ransomware Attacks

Ayed Al Qartah

Security Technical Solutions Architect
Cisco Systems

Attack landscape constantly evolving



Advanced Persistent Threats

Unpatched Software

Spyware/Malware

Wiper Attacks

Phishing

Man in the Middle

DDoS

Cryptomining

Supply chain attacks

Ransomware

Data/IP Theft

Malvertising

Drive by Downloads

Rogue Software

Botnets

Credential compromise



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

Cleveland Hopkins Airport affected by ransomware attack

Cleveland Hopkins International Airport has been target of more cyber attacks, but security upgrades blocked them

Cyber attack led to Bristol Airport blank screens

Louisville Regional Airport Authority grounded by ransomware attack

Airports are ill-equipped to deal with a major cyber attack, says consultancy firm

Kolkata: 4,000 flyers stranded as cyber attack led to delay of 30 flights

The World's Busiest Airport Shuts off Wi-Fi Amid a Ransomware Attack

Ukraine govt, banks & airports hit by mass ransomware attack

Ukraine says to review cyber defences after airport targeted from Russia



Aviation Cybersecurity: Major Challenges





Key assets supporting the daily airport operation

- **IT and Communications including internal and external infrastructure:**
 - Internal: Lan, VPN, IT equipment, Mobile network and apps, passenger WIFI, SOC, Flight Display Systems.
 - GPS, cloud-based data, Network Security Management, WAN, Air to satellite communication systems, GIS, etc.
- **Airline / Airside Operations:** including among others – air traffic management, flight tracking systems, departure control systems, airfield lighting and runway control and monitoring, cargo processing, aircraft re-fuelling, etc.
- **Landside Operations:** including the landside operations systems control center, fuel management, lighting detection systems, parking management systems, etc.
- **Safety and Security:** access control systems, authentication systems, baggage screening and handling systems, surveillance systems, passenger screening, perimeter intrusion detection, emergency response, firefighting, etc.



Key assets supporting the daily airport operation – cont.

- **Customer Ancillary Services:** Cashpoint terminals, mobile payments, point of sales (PoS), duty free, catering, etc.
- **Facilities and Maintenance:** airport vehicle maintenance, building management and control systems, energy management systems, lifts and escalators, SCADA (utilities, roads, ancillary areas), environmental management systems, etc.
- **Passenger Management Systems:** kiosk devices, e-ticketing, electronic visual information display systems, passenger check-in and boarding, central reservation systems, etc.
- **Staff Management:** staff records management, authentication systems, mobility-enabled applications.



Taxonomy of threats to the cyber security of Smart airports





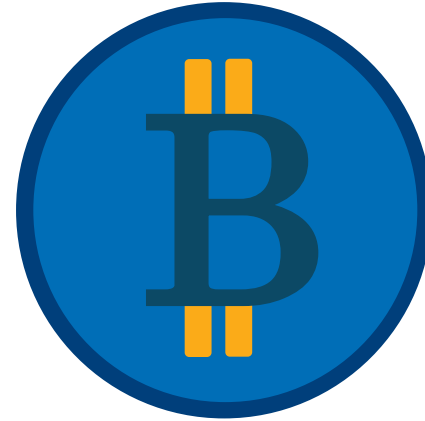
Ransomware



Malicious
Software



Encrypts
Critical Data

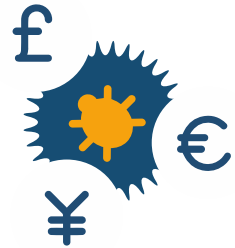


Demands
Payment



Ransomware

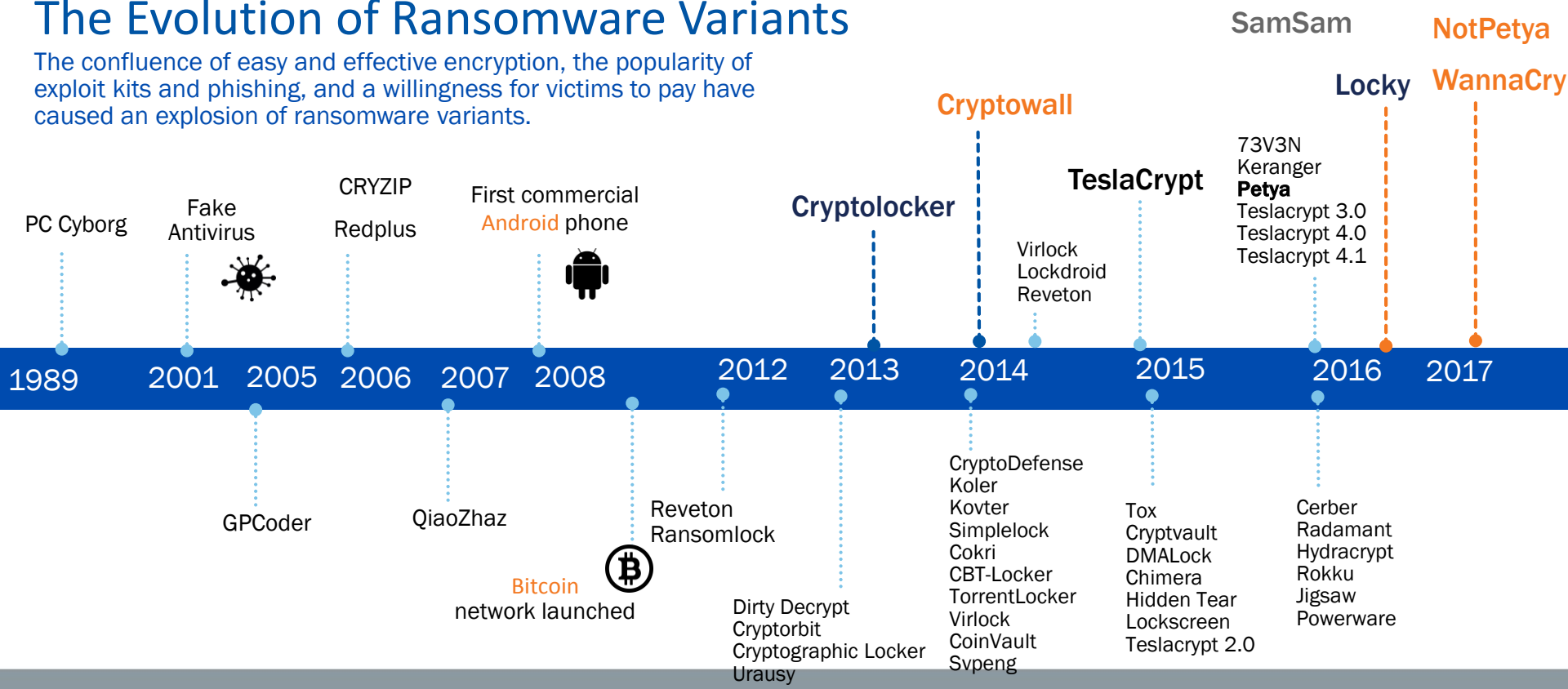
- Ransomware is the most profitable type of malware in history.
- Ransomware has changed the game from stealthy undetected access to extortion.
- Ransomware uses traditional malware attack vectors such as phishing emails, known vulnerabilities, and exploit kits to deliver the ransomware to a desktop.
- Ransomware communications include command and control (C2) callback methods for obtaining encryption keys and payment messaging are mostly using DNS.





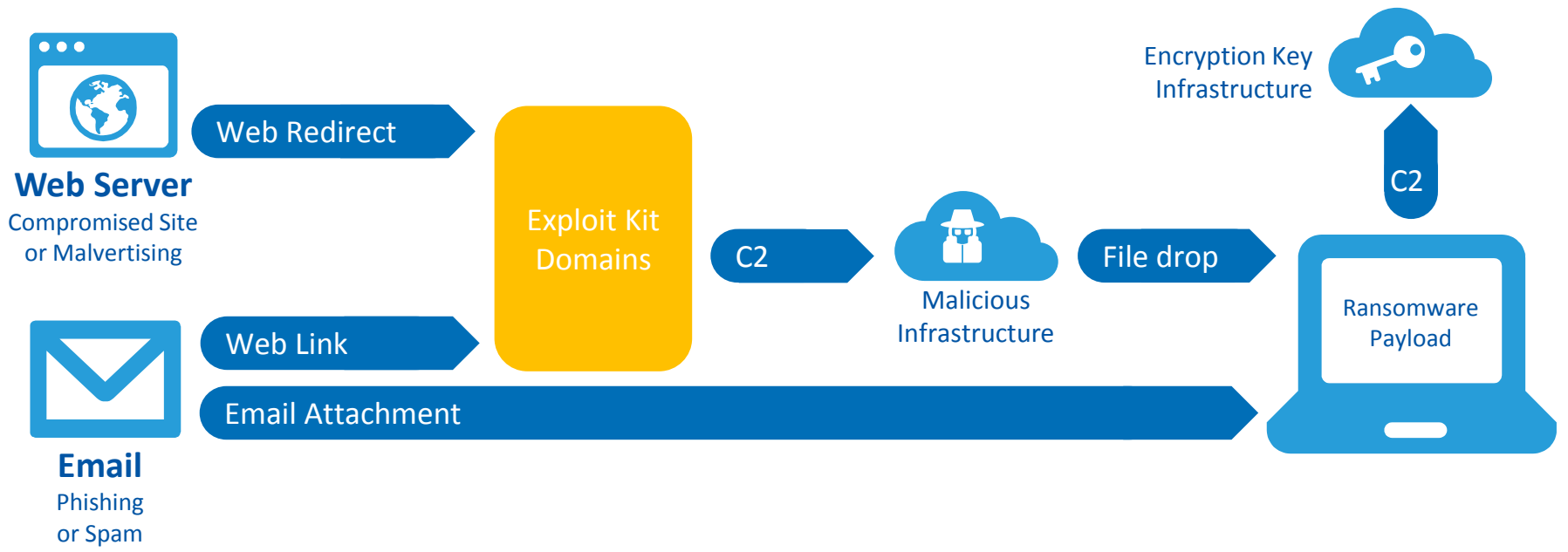
The Evolution of Ransomware Variants

The confluence of easy and effective encryption, the popularity of exploit kits and phishing, and a willingness for victims to pay have caused an explosion of ransomware variants.





Ransomware Email and Web Delivery

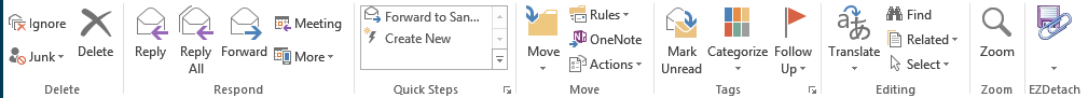




Ransomware and DNS

NAME*	Encryption Key				Payment MSG
	DNS	IP	NO C2	TOR	PAYMENT
Locky	●	●			DNS
SamSam			●		DNS (TOR)
TeslaCrypt	●				DNS
CryptoWall	●				DNS
TorrentLocker	●				DNS
PadCrypt	●				DNS (TOR)
CTB-Locker	●			●	DNS
FAKBEN	●				DNS (TOR)
PayCrypt	●				DNS
KeyRanger	●			●	DNS

FILE MESSAGE



Tue 12/12/2017 11:30

Amazon Marketplace <lqftdwbmxYYft@marketplace.amazon.com>

Invoice RE-2017-12-12-00572

To victim@victimsdomain.com

Message RE-2017-12-12-00572.doc (157 KB)

----- Begin message -----

Dear customer,

We want to use this opportunity to first say "Thank you very much for your purchase!"

Attached to this email you will find your invoice.

Kindest of regards,
your Amazon Marketplace

==

G [commMgrHmdToken:GJARWGBKYBKON]

----- End message -----

P For Your Information: To help arbitrate disputes and preserve trust and safety, we retain all messages buyers and sellers send through Amazon.com. This includes your response to the message below. For your protection we recommend that you only communicate with buyers and sellers using this method.

R Important: Amazon.com's A-to-z Guarantee only covers third-party purchases paid for through our Amazon Payments system via our Shopping Cart or 1-Click. Our Guarantee does not cover any payments that occur off Amazon.com including wire transfers, money orders, cash, check, or off-site credit card transactions.

Ic [commMgrTok:GJARWGBKYBKON]



Zoom

Zoom

es related to tax procedures, arrears, and payments, etc.

e is the tax debt for your realty - the realty tax. Ordinarily, such a way, we must take relevant measures to remedy

ull information regarding realty tax accrual, your debt

ur tax manager and provide them with the



Doops, your important files are encrypted.

If you see this text, then your files are no longer accessible, because they have been encrypted. Perhaps you are busy looking for a way to recover your files, but don't waste your time. Nobody can recover your files without our decryption service.

We guarantee that you can recover all your files safely and easily. All you need to do is submit the payment and purchase the decryption key.

Please follow the instructions:

1. Send \$300 worth of Bitcoin to following address:

1Mz7 [QR code] BWX

2. Send your Bitcoin wallet ID and personal installation key to e-mail wowsmith123456@posteo.net. Your personal installation key:

Njj [QR code] P5

If you already purchased your key, please enter it below.

Key:

Oops, your important files are encrypted.

If you see this text, then your files are no longer accessible, because they have been encrypted. Perhaps you are busy looking for a way to recover your files, but don't waste your time. Nobody can recover your files without our decryption service.

We guarantee that you can recover all your files safely and easily. All you need to do is submit the payment and purchase the decryption key.

Please follow the instructions:

1. Send \$300 worth of Bitcoin to following address:
1Mz75330mKfzR2R1t78mGSdzaAtNbBX
2. Send your Bitcoin wallet ID and personal installation key to e-mail www@1h123456@posteo.net. Your personal installation key:
RYS6IZ-2z6cuz-8BjpcF-pqD0z-qMCA5-nd8XK-876pA-5jT1e-2J9AKx-2CS8Kx

If you already purchased your key, please enter it below.
Key: _____



Oops, your important files are encrypted.

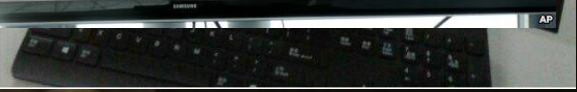
If you see this text, then your files are no longer accessible, because they have been encrypted. Perhaps you are busy looking for a way to recover your files, but don't waste your time. Nobody can recover your files without our decryption service.

We guarantee that you can recover all your files safely and easily. All you need to do is submit the payment and purchase the decryption key.

Please follow the instructions:

1. Send \$300 worth of Bitcoin to following address:
1Mz75330mKfzR2R1t78mGSdzaAtNbBX
2. Send your Bitcoin wallet ID and personal installation key to e-mail www@1h123456@posteo.net. Your personal installation key:
RYS6IZ-2z6cuz-8BjpcF-pqD0z-qMCA5-nd8XK-876pA-5jT1e-2J9AKx-2CS8Kx

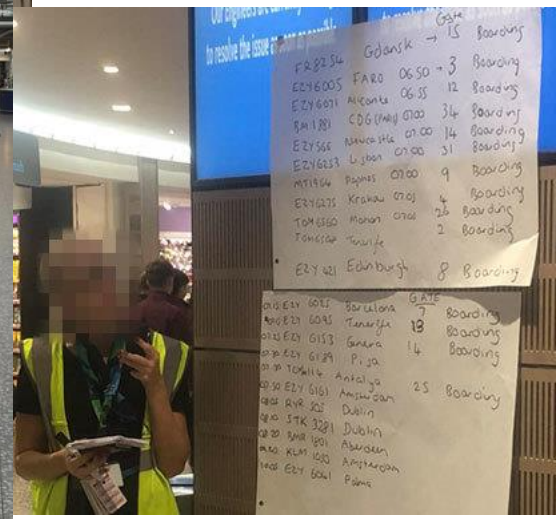
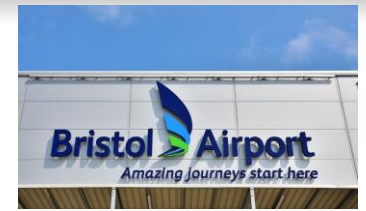
If you already purchased your key, please enter it below.
Key: _____



Bristol Airport Ran



2018





Capabilities needed to break the kill chain



- Threat intelligence – Knowledge of existing Ransomware and communication vectors



- E-mail security – Block Ransomware attachments and links



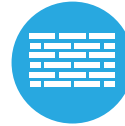
- Web Security – Block web communication to infected sites and files



- DNS Security - Break the Command & Control call back



- Client Security – Inspect files for Ransomware and Virus's, quarantine and remove



- Segment infrastructure – Authenticate access, separate traffic based on role and policy



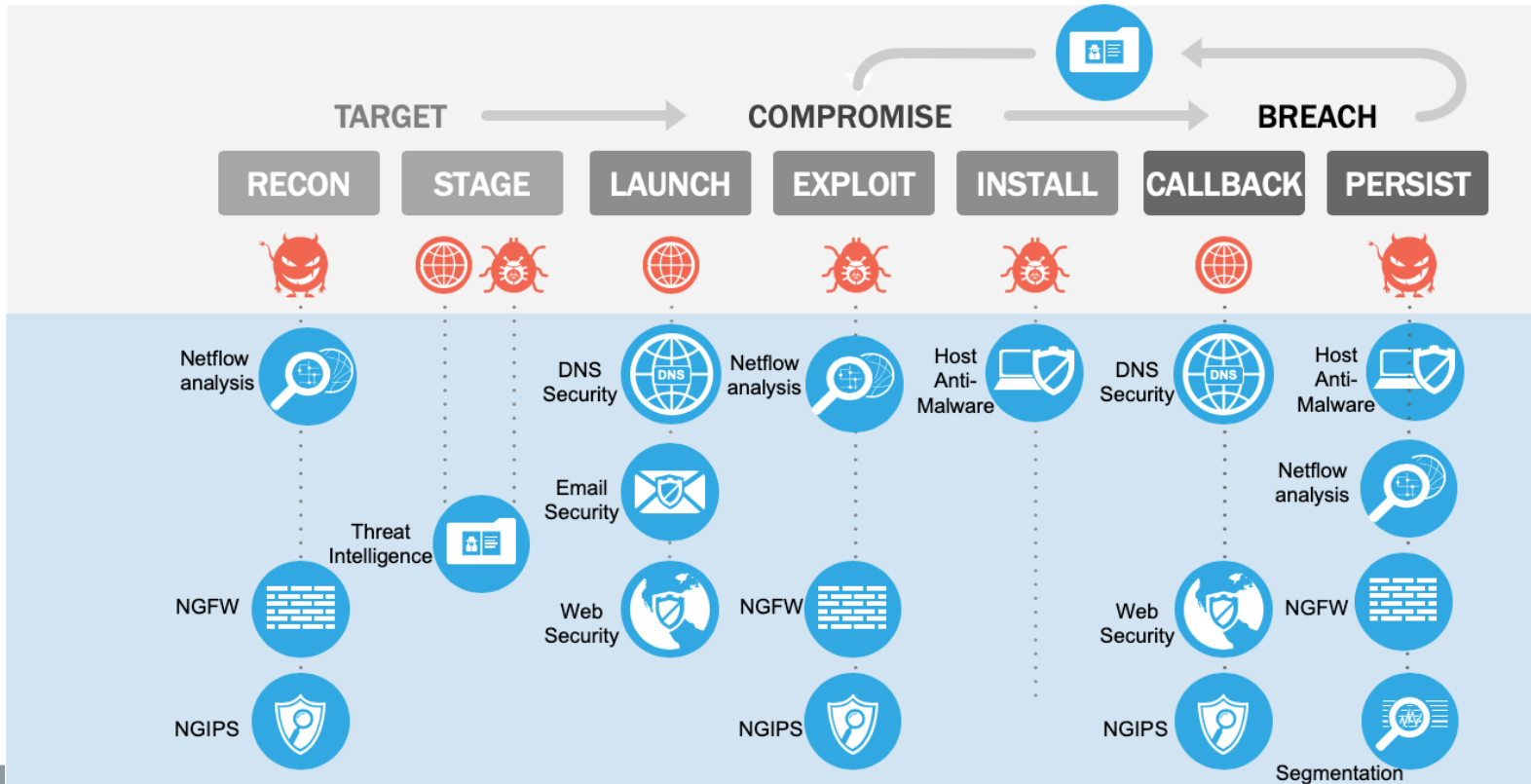
- Intrusion Prevention - Block attacks, exploitation and intelligence gathering



- Monitor Infrastructure communications – Identify and alert on abnormal traffic flows



Capability Defense against the “Kill Chain”





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

Final thoughts

- Commercial airlines and other transportation providers present a tempting target for cybercriminals
- As technology adoption evolves in the civil aviation industry, it will have to invest in smarter, safer digital infrastructure that leverages machine learning, integrated cyber security architecture, and threat intelligence to thwart attacks and ensure that its critical systems are protected and always available.



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

Questions?





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



ICAO

North American
Central American
and Caribbean
[NACC] Office
Mexico City

South American
[SAM] Office
Lima

ICAO
Headquarters
Montréal

Western and
Central African
[WACAF] Office
Dakar

European and
North Atlantic
[EUR/NAT] Office
Paris

Middle East
[MID] Office
Cairo

Eastern and
Southern African
[ESAF] Office
Nairobi

Asia and Pacific
[APAC] Sub-office
Beijing

Asia and Pacific
[APAC] Office
Bangkok



THANK YOU



ICAO 2019

75 YEARS OF CONNECTING THE WORLD

الإيكاو ٢٠١٩

٧٥ عاماً

من الربط بين أرجاء العالم

