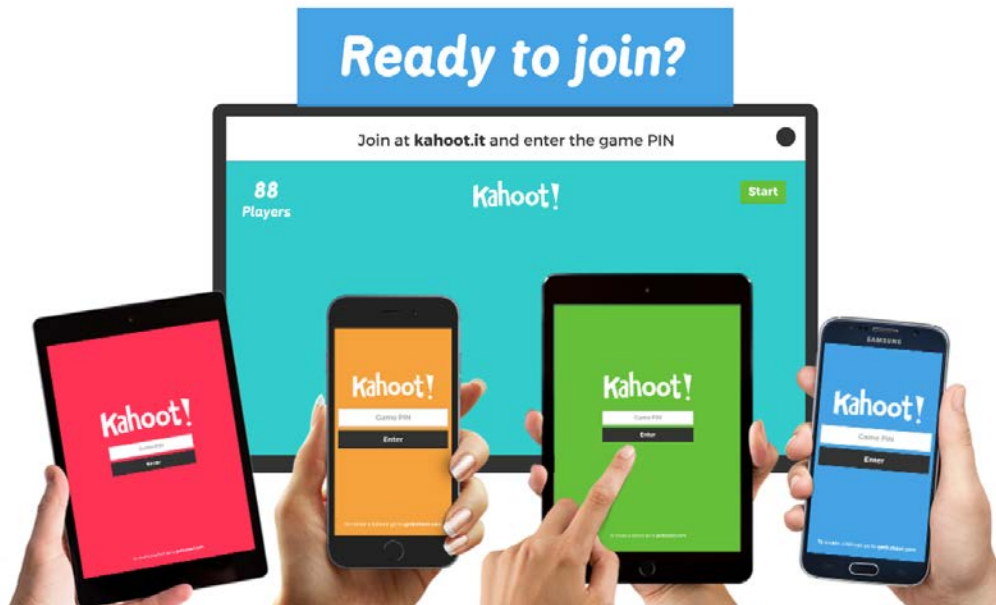


# Cyber/PCI Session Game:

Join with the **Kahoot! app** or at **kahoot.it**  
with Game PIN:

**126666**



## Airport Cyber Security & PCI Compliance

Play with the new Kahoot! app



# Agenda

- Kahoot! Cyber / PCI Game
- Overview / Panel
- PCI-DSS SAQs Review
- Cyber Security Trends
- Cyber Focus Areas
- Resources

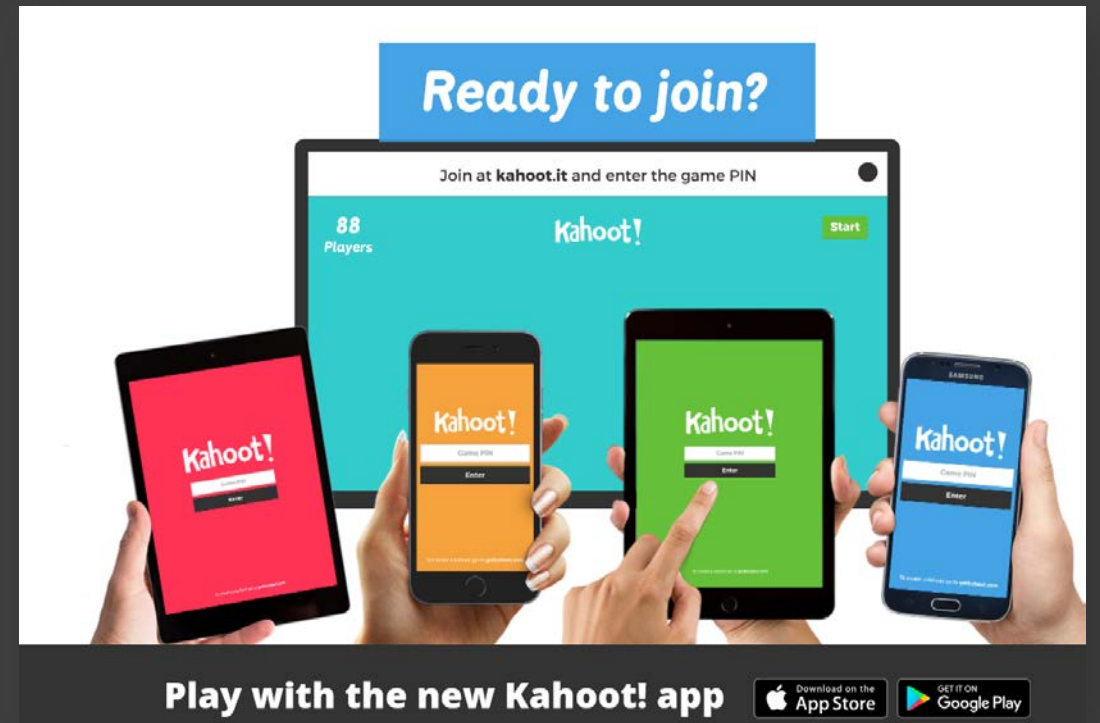


# Cyber/PCI Session Game:

Join with the **Kahoot! app** or at **kahoot.it**  
with Game PIN:

**126666**

# Let's play the game!



The image shows a promotional graphic for the Kahoot! app. At the top, a blue banner reads "Ready to join?". Below it, a large tablet displays the Kahoot! website interface, showing "88 Players" and a "Start" button. In front of the tablet are four mobile devices (two tablets and two smartphones) held by hands, each displaying the Kahoot! app interface with a "Game PIN" input field and an "Enter" button. The devices have different colored backgrounds: red, orange, green, and blue. At the bottom, a dark grey banner contains the text "Play with the new Kahoot! app" and logos for the App Store and Google Play.

Ready to join?

Join at **kahoot.it** and enter the game PIN

88 Players

Kahoot!

Start

Kahoot!

Game PIN

Enter

Kahoot!

Game PIN

Enter

Kahoot!

Game PIN

Enter

Kahoot!

Game PIN

Enter

Play with the new Kahoot! app

Download on the App Store

GET IT ON Google Play

# Overview

- **Cybersecurity** remains a high priority for both airport and airline CIOs, with spending projected at nearly \$4B in 2018.
- **Payment Card Industry Data Security Standard (PCI DSS)** is an important topic for airport operators.
- Also, learn more about how the **ACI Cybersecurity Task Force** is working to expedite more effective industry safeguards.

## Panel Introduction & Talking Points

### **Dom Nessi, VP/Strategic Engagement A-ISAC**

- State and Federal IT and Cyber knowledge
- New threats and threat intelligence
- Airport IT attack surface

### **Daver Malik, ACIO Phoenix Sky Harbor Intl.**

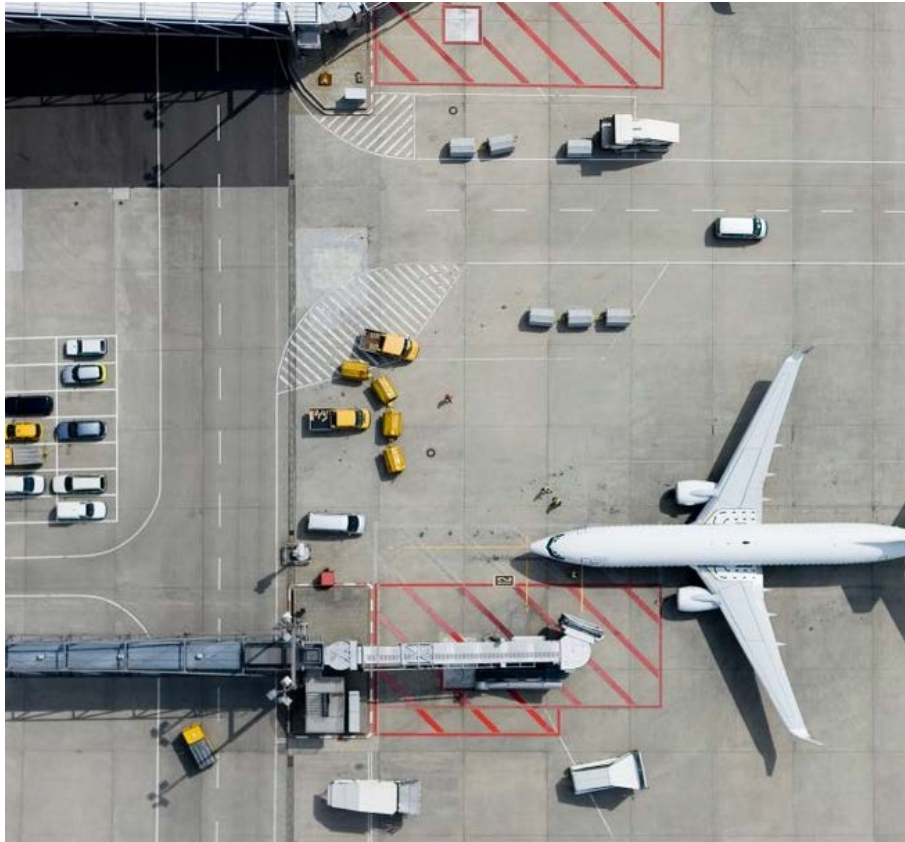
- Airport & Private Sector Aviation knowledge
- Technology and Digital Strategy

### **Phillip Murray, IT Director Southwest Florida Intl. Airport**

- Airport specific PCI/Cyber knowledge
- PCI-DSS Strategy and Timeline

### **Royce Holden, AVP ITS (CISO) DFW Intl. Airport**

- Airport IT and Cyber knowledge
- Governance, Risk and Compliance



Join this **Survey** with the **Kahoot!**  
**app** or at **kahoot.it**

with Game PIN:

**919914**



Kahoot! Question #1

---



## Discussion

*... Given your background & experience, how have you dealt with PCI compliance?*





Kahoot! Question #2

## Examples: Fixed-based Operators (FBOs)

SAQ	DESCRIPTION	NUMBER OF QUESTIONS	VULNERABILITY SCAN	PENETRATION TESTING
A	<b>E-commerce website (third party)</b> <ul style="list-style-type: none"> <li>Fully outsourced card acceptance and processing</li> <li>Merchant website provides an iframe or URL that redirects a consumer to a third-party payment processor</li> <li>Merchant cannot impact the security of the payment transaction</li> </ul>	22	N	N
A-EP	<b>E-commerce website (direct post)</b> <ul style="list-style-type: none"> <li>Merchant website accepts payment using direct post or transparent redirect service</li> </ul>	191	Y	Y
B	<b>Processes cards via:</b> <ul style="list-style-type: none"> <li>Analog phone, fax, or stand-alone terminal</li> <li>Cellular phone (voice), or stand-alone terminal</li> <li>Knuckle buster/imprint machine</li> </ul>	41	N	N
B-IP	<b>Processes cards via:</b> <ul style="list-style-type: none"> <li>Internet-based stand-alone terminal isolated from other devices on the network</li> </ul>	82	Y	N



# Examples: Parking System (small/medium hub)

SAQ	DESCRIPTION	NUMBER OF QUESTIONS	VULNERABILITY SCAN	PENETRATION TESTING
C-VT	<b>Processes cards:</b> <ul style="list-style-type: none"><li>• One at a time via keyboard into a virtual terminal</li><li>• On an isolated network at one location</li><li>• No swipe device</li></ul>	79	N	N
C	<b>Payment application systems connected to the Internet:</b> <ul style="list-style-type: none"><li>• Virtual terminal (Not C-VT eligible)</li><li>• IP terminal (Not B-IP eligible)</li><li>• Mobile device (smartphone/tablet) with a card processing application or swipe device</li><li>• View or handle cardholder data via the Internet</li><li>• POS with tokenization</li></ul>	160	Y	N
D	<b>E-commerce website</b> <ul style="list-style-type: none"><li>• Merchant website accepts payment and does not use a direct post or transparent redirect service</li></ul> <b>Electronic storage of card data</b> <ul style="list-style-type: none"><li>• POS system not utilizing tokenization or P2PE</li><li>• Merchant stores card data electronically (email, e-fax, recorded calls, etc.)</li></ul>	329	Y	Y

SAQ	DESCRIPTION	NUMBER OF QUESTIONS	VULNERABILITY SCAN	PENETRATION TESTING
D	<b>E-commerce website</b> <ul style="list-style-type: none"> <li>• Merchant website accepts payment and does not use a direct post or transparent redirect service</li> </ul> <b>Electronic storage of card data</b> <ul style="list-style-type: none"> <li>• POS system not utilizing tokenization or P2PE</li> <li>• Merchant stores card data electronically (email, e-fax, recorded calls, etc.)</li> </ul>	329	Y	Y
P2PE	<b>Point-to-point encryption</b> <ul style="list-style-type: none"> <li>• Validated PCI P2PE hardware payment terminal solution only</li> <li>• Merchant specifies they qualify for the P2PE questionnaire</li> </ul>	33	N	N

Examples: Parking System (large hub)



Kahoot! Question #3

# Kahoot! Question #4




400	00
783	73
219	52
152	42
111	32

# RSW PCI Timeline

- Awareness - 2009
  - Assessment - 2010
  - Policy - 2011
  - Remove Storage - 2014
- 



# RSW PCI Timeline

- Begin PCI Network - 2015
  - Complete PCI Network - 2017
  - SAQ - 2018
  - Bi-Annual Security Assessments
- 



Discussion

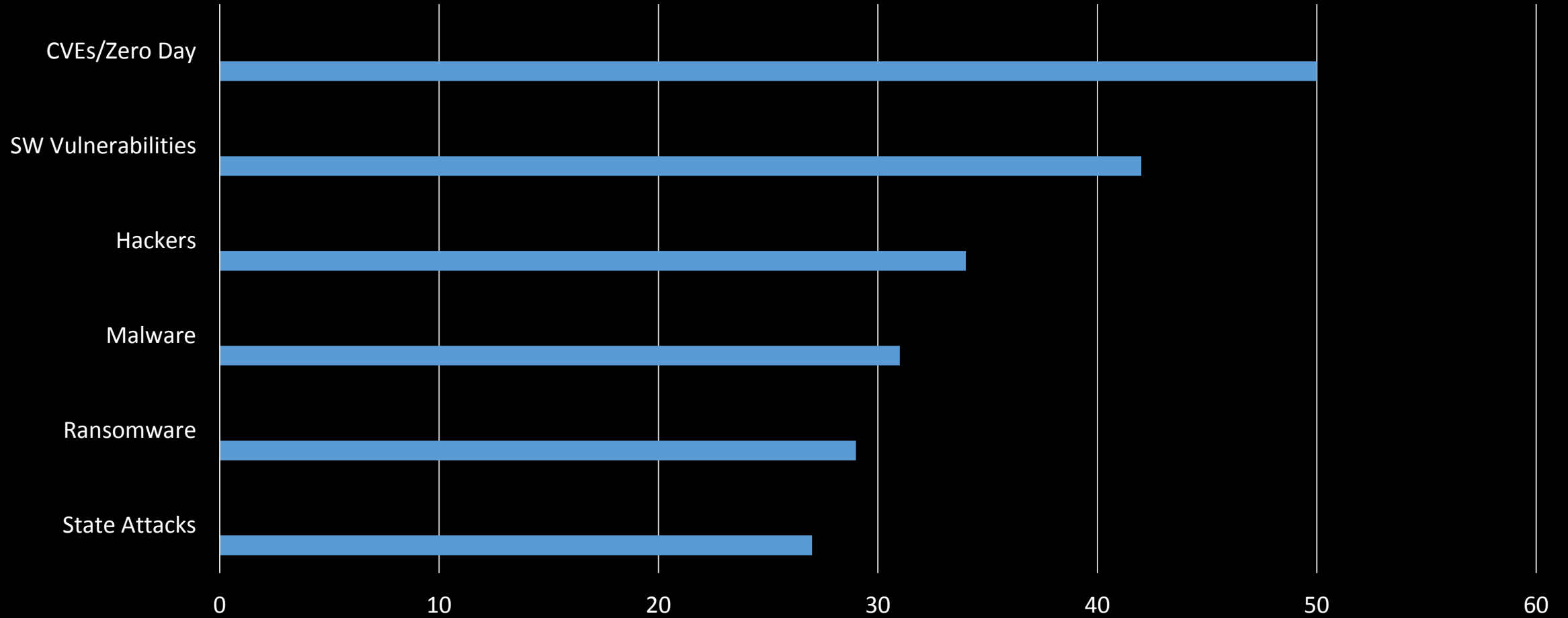
*...Switching gears,  
let's start where we  
should start: Cyber  
Security*

# Aviation – ISAC

Recent reported cyber threats  
(Jan. – March 2019)



# Most Common Major Threats Reported



# Threat Articles by Type – 64 days

Critical Vulnerabilities/ Zero Days	50	DDOS	15
Software Vulnerabilities	42	IoT/Infrastructure	12
Hackers	34	Email/BEC	9
Malware	31	APTs	9
Ransomware	29	Cloud	5
State Attacks	27	Mobile Devices	4
Privacy/Data Breach	21	RootKit	3
Phishing	19	Phones	3
Hardware	16	Web	3
		MalSpam	2
		Social Media	2





Total number of articles in A-ISAC DAM – 896

Total articles with specific threats – 336

Approximately 14 new threats reported daily



## In the News ...

Average cost of a cyberattack passes \$1 million

Japanese Government to urge infrastructure data for aviation sector be kept on domestic servers

NASA Examines Blockchain Tech to Secure Aircraft Flight Data

In the Cloud Era Why Do Government Websites Still Go Dark During Shutdowns?



## In the News ...

Researchers claim Pen Testers breach 92 percent of companies

Security vulnerabilities in **video conferencing devices** could be remotely exploited by hackers

**Digital sign systems** allowed hacker access through default passwords

**E-ticketing system** exposes airline passengers' personal information via email

Phishing Campaign Uses Fake Google reCAPTCHA to Distribute Malware



## Debunking Incorrect or Misleading Information

Chris Roberts Claims MH370 Lost due to 'Cyber hacking attack'

*The Aviation-ISAC is informing all stakeholders of the existence of this recent interview conducted with Chris Roberts. The Aviation ISAC deems this reporting to be irresponsible and inflammatory*



# **Biometric Advancements**

**Lufthansa launches biometric boarding at Miami International Airport**

**Vancouver Airport First to Update Border Control Solution to Canadian Government Biometric Requirements**

**Facial recognition technology will be rolled out at 20 major US airports by 2021**





## **AI May Soon Defeat Biometric Security** - *From IBM Security Intelligence* (01.31.2019) - *Mike Elgan*

Threat actors will soon gain access to artificial intelligence (AI) tools that will enable them to defeat multiple forms of authentication — from passwords to biometric security systems and even facial recognition software — identify targets on networks and evade detection.

And they'll be able to do all of this on a massive scale.

Threat actors will soon be able to simply go shopping on the dark web for the AI tools they need to automate new kinds of attacks at unprecedented scales.



## FBI arrests second Apophis Squad hacker in the US, who targeted LAX

The FBI arrested yesterday a hacker part of a hacking team known as Apophis Squad

- Two persons, US and UK citizens, respectively, have been charged in an indictment unsealed by the US Department of Justice yesterday.
- Orchestrated a crime spree during the first eight months of 2018
- Allegedly launched DDoS attacks against online websites, made phone calls and sent email threats to schools, government agencies, and airports containing bogus reports of physical violence, mass-shootings, and bomb threats.



## ICAO tried to cover up 2016 cyberattack by China APT Group - *From CBC News (02.27.2019) Debra Arbec*

November 2016, the Montreal-based International Civil Aviation Organization (ICAO) was hit by the most serious cyberattack in its history

- Internal documents suggest key members of the team that should have prevented the attack tried to cover up how badly it was mishandled
- ICAO is the gateway to everyone in the aviation industry, so an uncontained cyberattack left not just ICAO vulnerable, but made sitting ducks of its partners worldwide
- The hacker was most likely a member of Emissary Panda, a sophisticated and stealthy espionage group with ties to the Chinese government



- Investigators found a network full of holes, with security vulnerabilities that should have been flagged years earlier
- Assessment reports show that a cyber-intelligence analyst working for the **Aviation Information Sharing and Analysis Center** first flagged the cyberattack on Nov. 22, 2016
- “Watering hole” attack, in which hackers find a website that their targets frequent and infect it with malware in order to gain access to those targets
- Within 30 minutes of the hack, at least one of the UN agency's 192 member states, Turkey, had been compromised



## Sydney Airport to implement major cyber security upgrades - *From TechGenix (03.04.2019) - Derek Kortepeter*

Airports, in particular, have had numerous incidents with cybercrime and some are stepping up their game in an attempt to mitigate the risk of coming under attack.

- According to an end-of-the-year summary report from Sydney Airport, the Australian transport hub is taking extra steps to try and prevent major hacking incidents.
- The most notable of these measures is a round-the-clock "Security Control Centre" that is expected to be completed in April, 2019
- The report describes the strategy as follows: “ ... We work closely with the Australian government via the Joint Cyber Security Centre (JCSC) and are partnering with the **Aviation Information Sharing and Analysis Centre (A-ISAC)** on global aviation cyber security intelligence. “





# ACI-WORLD UPDATE

---



**AIRPORTS COUNCIL  
INTERNATIONAL**



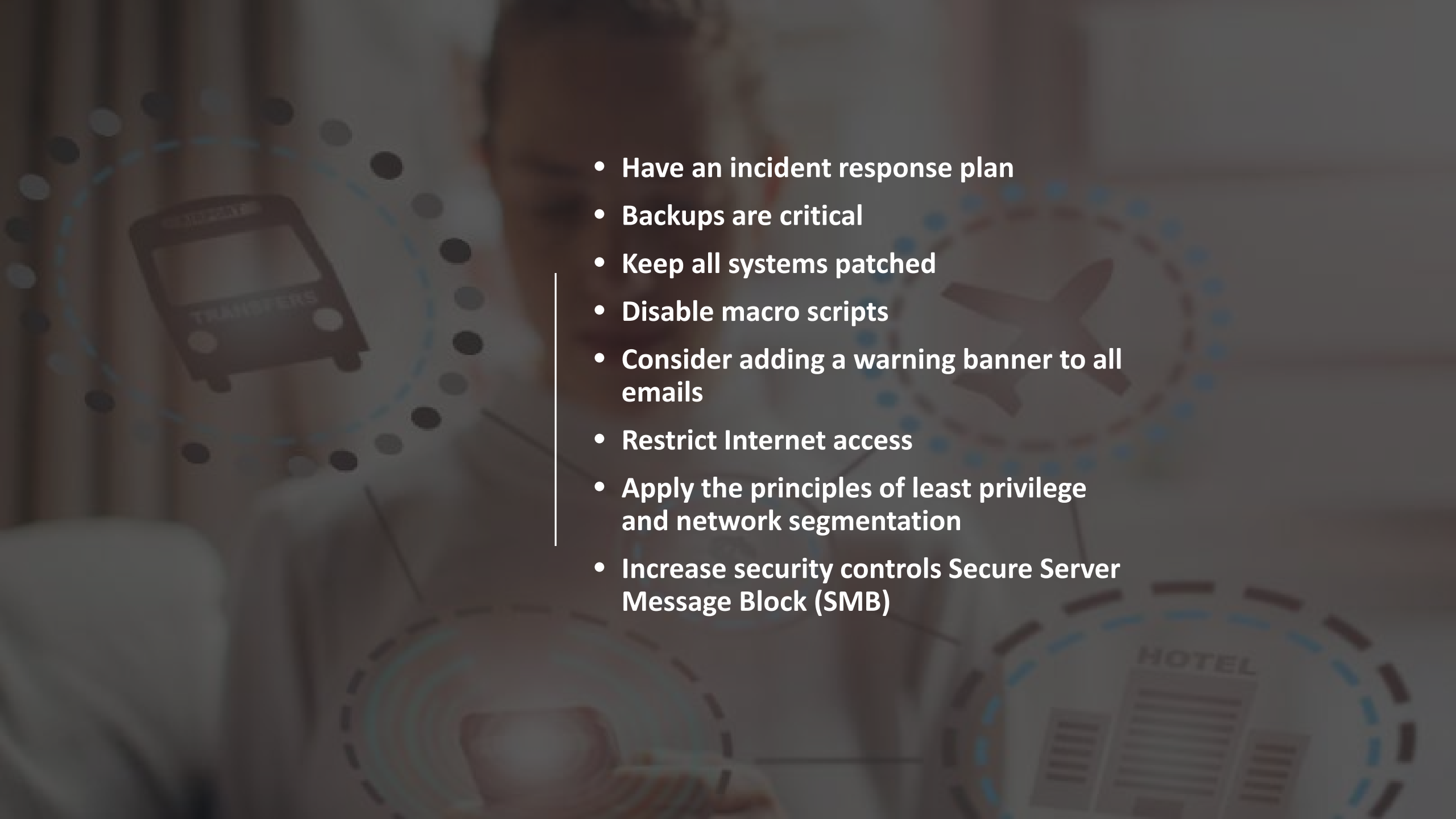
Kahoot! Question #5





## Discussion

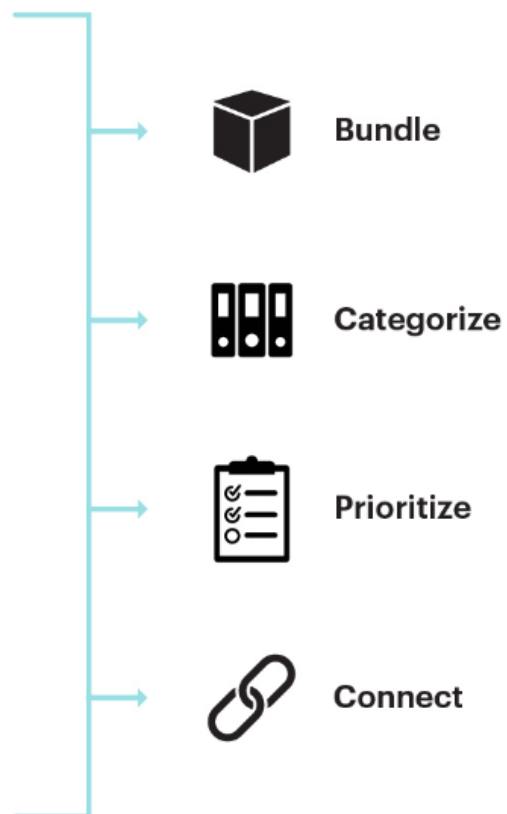
*... with an ever-changing cyber security landscape, how do you address the challenge with executives?*

- 
- Have an incident response plan
  - Backups are critical
  - Keep all systems patched
  - Disable macro scripts
  - Consider adding a warning banner to all emails
  - Restrict Internet access
  - Apply the principles of least privilege and network segmentation
  - Increase security controls Secure Server Message Block (SMB)

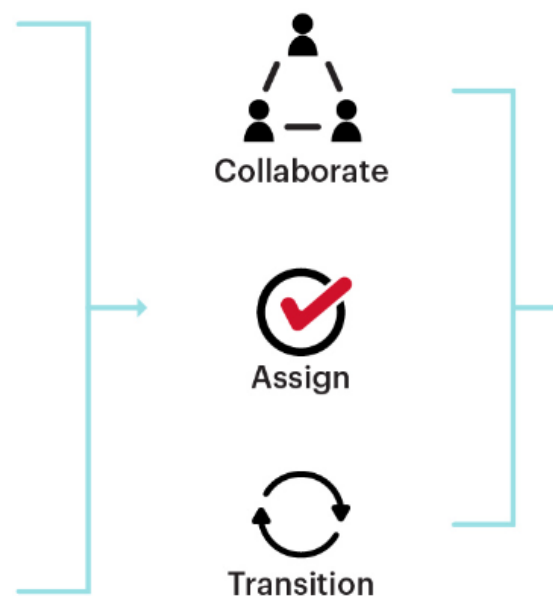
## COLLECT



## ALERT



## INVESTIGATE



## RESPOND







## Discussion

*... Airports are at different stages of cyber security maturity. How do you handle benchmarking?*

## Results generated for sample Test Airport:

Section	Domain description	# Ctrls	# Completed	N/A	Compliance %	Capability level	Description	
5	<a href="#">5. Security Policy</a>	3	3	0	🟡	66%	1	Performed
6	<a href="#">6. Organization Of IS</a>	7	7	0	🟡	71%	1	Performed
7	<a href="#">7. Assest Management</a>	3	3	0	🟡	66%	2	Managed
8	<a href="#">8. HR Security</a>	8	8	0	🔴	12%	2	Managed
9	<a href="#">9. Physical &amp; Env. Security</a>	11	11	0	🔴	9%	2	Managed
10	<a href="#">10. Comms. &amp; Ops. Management</a>	25	25	1	🔴	24%	2	Managed
11	<a href="#">11. Access Control</a>	19	19	1	🔴	10%	1	Performed
12	<a href="#">12. Systems Aquisitions, D&amp;M</a>	15	15	0	🔴	20%	2	Managed
13	<a href="#">13. Incident Management</a>	4	4	0	🔴	25%	1	Performed
14	<a href="#">14. Businesss Continuity</a>	7	7	0	🔴	14%	1	Performed
15	<a href="#">15. Compliance</a>	10	10	0	🔴	10%	1	Performed
Results:					🔴	29.73%	Level 1	Performed



**FREE  
WI-FI**



Connect to:  
TransitWirelessWiFi

Transit **WI-FI**

Kahoot! Question #6





Kahoot! Question #7

# Resources

- A-ISAC - <https://www.a-isac.com/>
- Center for Internet Security (CIS) - <https://www.cisecurity.org/white-papers/ms-isac-security-primer-ransomware/>
- National Safe Skies Alliance –Cyber Risk Assessment Tool + Quick Guide (0070) <https://www.sskies.org/paras/reports/>
- FISMApedia – Collection of FISMA and other Federal IT Security and Assurance Programs:
  - [http://fismapedia.org/index.php/Main\\_Page](http://fismapedia.org/index.php/Main_Page)