Raising the Profile of Cyber Risk at Airports

Questions and considerations around organizational support for cybersecurity

CYPRUS LAKE
Revolutionizing Cyber Risk™

Matt Crowley, CM, CISSP
matt@cypruslake.com
(216) 337-7625

Important Question

Which airport employee
should be fired after
a cyber breach?

State of Cyber@ US Airports

- **Good progress** in the industry
  - ACI BIT and Cyber Security Task Force
  - Greater support from federal government
  - Increase in services, training, testing
  - Greater knowledge sharing
  - Introduction of standardized frameworks

- Problems Remain
  - **Severity**, **Scope**, and **Support**

State of Cyber@ US Airports - Severity

- **Target on our backs**
- **2/3** of ransomware attacks: **gov't agencies**
- **75+ state and local** agencies in 2019 (so far)
  - Given that most US airports are local/state owned…

- **MSPs** now a major target
- Ever-shifting threat landscape

State of Cyber@ US Airports - Scope

- Hard to scale full programs to smaller airports
- Implementation highly variable
  - No industry-wide standard
  - Differences based on size/funding/ownership
- No mandate
  - No airport-specific cyber laws and regs
  - State laws variable
- Minimal 3rd Party Risk Management

State of Cyber@ US Airports - Support

- **Conversation still being led by IT**
- Lack of internal support
- **Minimal understanding** of issue
- **Tension** between departments
- **Unrealistic expectations**

Who's Accountable?

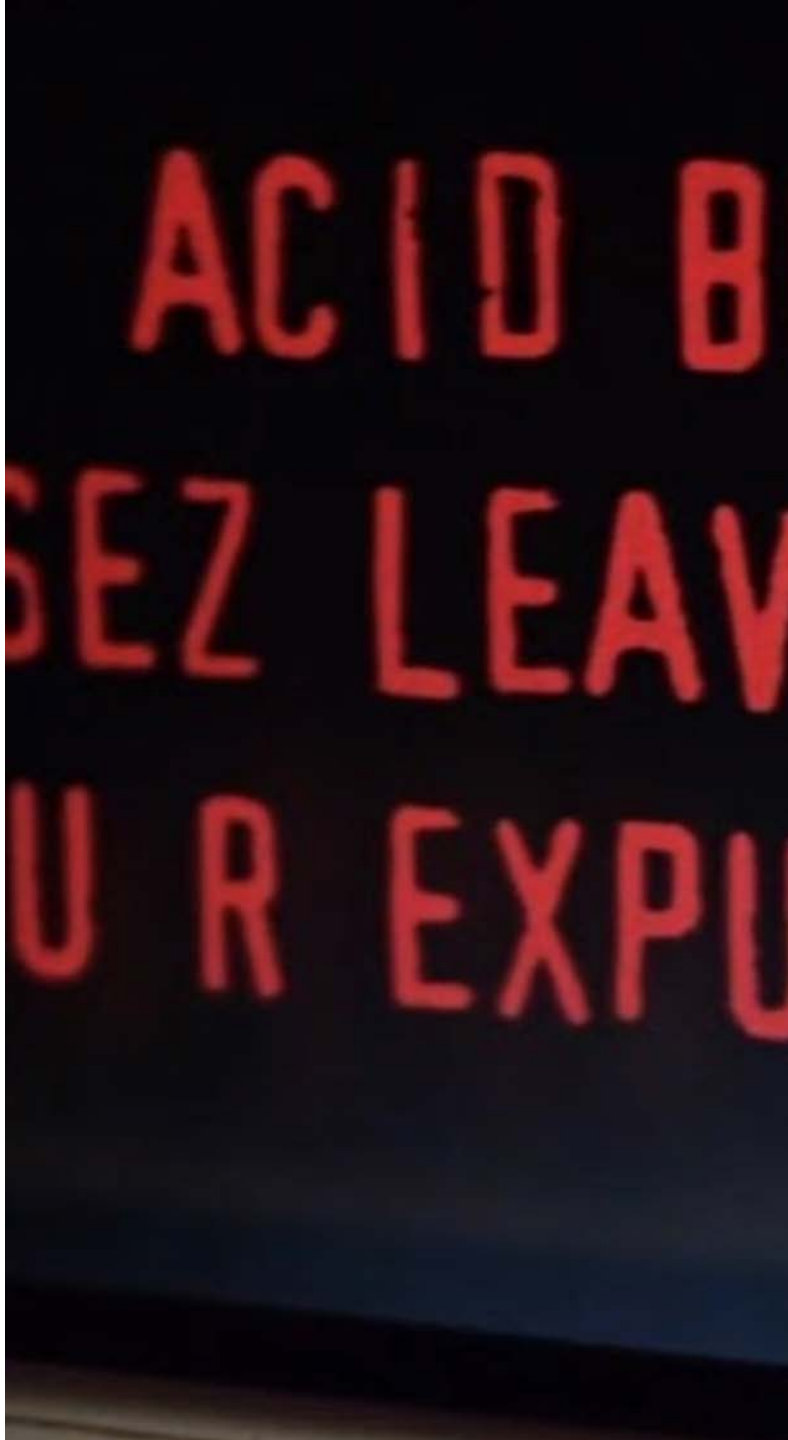
- Ultimately, the **CEO or Director is**
- Cyber risk management determined by:
  - Laws and regulations (a must!)
  - Strategic plans and strategic intent
- ***Business*** defines what must be protected
- Loses effectiveness in reverse:
  - No organizational buy-in
  - Might be addressing the wrong risks
  - Unnecessarily impacting lines of business

Who's Responsible?

- **Management must implement**
- "Security is everyone's responsibility…"
  - Not simply about reporting phishing emails
  - Data Owners vs System Owners
  - Classification
  - **Co-development** of policy and controls
  - Continual testing
- **Silos and politics need to be put aside**
- Concept of **cyber-physical convergence**

Important Question

Should the CIO be able to unilaterally override the CISO?



Who's In Charge?

- There **must** be a cybersecurity team
  - That can take many forms
  - Internal hires, managed services
- **The tension between cybersecurity and IT**
- The "CISO of 2019" is the "CIO of 1999"
  - Should cybersecurity team report into IT?
- Rise of the CSO at airports?
  - Back to the concept of cyber-physical convergence

In Summary

- Continually evolve, control, test
- Raise the conversation beyond IT
- Get business leaders to own the risk
- Gain control of your 3rd party risk
- Break down silos and co-develop
- Consider modern org structures
- Standardize industry before it's forced upon us