A PROACTIVE APPROACH TO CYBERSECURITY

ADDRESSING THE BASICS

ACI Workshop
Michael Zaddach, Munich Airport
Dom Nessi, former LAX CIO

Cybersecurity Today

- Most Large Airports have made at least some effort to secure their data and systems
- A subset of those have made extensive inroads into cybersecurity
- Many Small and Medium sized airports are aware of the threats but not sure what to do and where to start

The Normal Reaction – Protecting the Obvious

Many organizations consider cybersecurity solely a technology issue

- Having a security consultant conduct a review
- Penetration Testing
- Purchase firewalls, IDS, and IPS Hardware
- Attend conferences for an idea of what to do

The Normal Reaction – Protecting the Obvious

- While helpful, it does not establish a cybersecurity program
- Does not guarantee a holistic view of the cybersecurity measures needed for your organization
- **And does not promote assurance that you are safer**

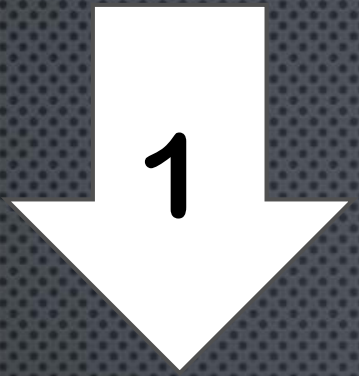
Handling the basics

Top – Down

and

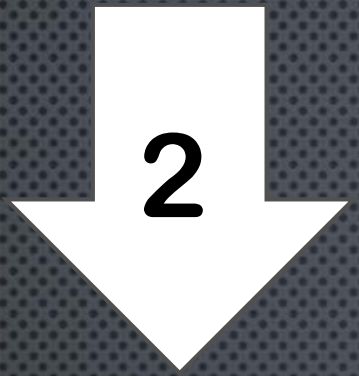
Bottom - Up

TOP - DOWN



- It Starts with **Governance** – an organization cannot properly secure itself until **top management** resolves itself to understand the threat and make the commitment to mitigate the most likely attacks
  - Create an internal cross-cutting organization responsible for cybersecurity
  - Membership includes Human resources, Finance, Public Safety, Legal Counsel, Operations, Facilities and, of course, Information Technology
  - Must meet at least semi-annually; and more frequently in the beginning

TOP - DOWN



- While it is not necessary for the Cybersecurity Governance Committee to be experts on cybersecurity, a basic level of **EDUCATION** is necessary
- Education separates reality from fiction
- Provides the entire committee with a foundation from which to set a goal, establish
- Focus on the CIA Triad – Confidentiality. Integrity and Availability

TOP - DOWN

Choose a **Framework** – Though this seems like a complex task, it is not

There are many frameworks available, the most likely ISO 27000

- It Provides A target to reach and guidance on what to do
- Take a baseline measurement against the Benchmark
- Use the ACI IT Security Benchmarking Tool

TOP - DOWN

4

- Commit to a **Risk Management** approach
- Have a third party conduct a thorough risk assessment
- Identify the threats and the vulnerabilities that are specific to the organization
- Determine the likelihood and impact of each threat

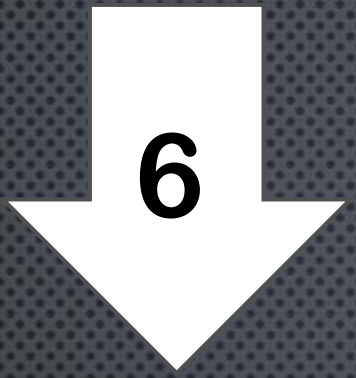
TOP - DOWN

5

Security Governance Committee Oversees Risk Assessment Results

- Identify a **Reasonable response** to each threat: mitigation, acceptance, avoidance, transfer, assignment
- Prioritize response actions
- Determine responsibility, schedule and funding

TOP - DOWN



Airport Management must be cognizant of the need for the following:

- Business Continuity (COOP)
- Disaster recovery (DR)

Should a cyberattack occur which hampers airport operational ability, a response must be established before it occurs

The COOP and DR must be tested periodically

TOP - DOWN 7

Review Risk management Policies and Determine the Need for Additional **Cyber Insurance**

- Protect your own organization
- Protect third parties
- Coverage to handle the response to a cyber attack

BOTTOM - UP

Intensive **Employee Awareness** Training

- Conducted at Least Annually
- Targeted to the Threats in that organization's specific environment
- Monthly email reminders
- Focus on Passwords, Mobile Devices, Social Engineering and Email
- Change the training contents every time it is delivered

BOTTOM - UP

Intensive **IT Employee Training**

- Conducted at Least Quarterly
- Includes all IT Employees – Not just those charged with Cybersecurity responsibilities
- Must be thorough and Comprehensive – Full coverage of all technology components
- May also include select non-IT employees

BOTTOM - UP 3

Empower Organizational **Cybersecurity Team**

- Identify a Chief Information Security Officer (CISO) as either a full-time (preferably) or priority duty
- Have Certified IT Cybersecurity professionals available
- Create a cyber-attack response team

BOTTOM - UP

Conduct a periodic "**LOCK-DOWN**" Exercise

- IT Environments change daily
- Every IT Employee must review EVERYTHING in their own immediate environment on a continual basis
- Identify potential threat vectors
- Document Issues
- Adopt new processes and procedures
- Take immediate action to close obvious holes
- Insure that virus detection software is up-to-date
- Think technology HYGEINE

BOTTOM - UP 5

DEVELOP A COMPREHENSIVE **INVENTORY** OF IT ASSETS

- DEVELOP AN UP-TO-DATE INVENTORY OF ALL PRODUCTION SYSTEMS, INCLUDING OS TYPES (AND VERSIONS), IP ADDRESSES, PHYSICAL LOCATION, CUSTODIAN AND FUNCTION.
- AUTOMATE THE INVENTORY USING A BASIC IT INVENTORY SYSTEM

BOTTOM - UP

Implement a **Formal Patch Program**

- Goes beyond installing patches as they occur
- Proper Patch Management includes:
  - Devise a plan for standardizing production systems to the same version of OS and application software.
  - Make a list of all the security controls you have in place--routers, firewalls, IDSes, AV, etc.--as well as their configurations.

BOTTOM - UP

Implement a **Formal Patch Program**

- Compare reported vulnerabilities against your inventory/control list. There are two key components to this. First, you need a reliable system for collecting vulnerability alerts. And second, you need to separate the vulnerabilities that affect your systems from those that don't.
- Classify the risk. Assess the vulnerability and likelihood of an attack in your environment
- Test the Patch, if Time Allows
- Apply the patch.

BOTTOM - UP 7

SECURE YOUR **PHYSICAL IT SPACE**

- OFTEN OVER-LOOKED IS PHYSICALLY SECURING IT SYSTEMS
- PHYSICAL ACCESS TO DATA CENTERS, TELECOMM ROOMS, AND IT INFRASTRUCTURE IS ESSENTIAL TO ENSURE AVAILABILITY
- TAKE A SPECIAL LOOK AT AIRPORT SECURITY SYSTEMS (CCTV, ACCESS CONTROL, ETC.)

SUMMARY

TOP DOWN

1. Governance
2. Education
3. Framework
4. Risk Management
5. Reasonable Response
6. Business Continuity – Disaster recovery
7. Cyber Insurance

BOTTOM UP

1. Security awareness Training
2. IT Employee Training
3. Empower Cybersecurity Team
4. Lock Down Exercise
5. Inventory
6. Formal Patch Program
7. Secure Physical Space

Questions and comments

Thank you for your attention