ACRP Report 140
Guidebook on Best Practices for Airport Cybersecurity

Randy Murphy
Principal Investigator

ACRP

AIRPORT COOPERATIVE RESEARCH PROGRAM

Research Team

- Randy Murphy, Principal Investigator
  - Founder Grafton Technologies, Inc.
  - Worked in aviation for over 24 years
  - Past 19 years focused on Airport IT
- Michael Sukkarieh
- SoftKrypt
  - Jon Haass
  - Paul Hriljac
- Grafton Information Services

Oversight Panel

- Royce Holden, Greater Asheville Regional Airport Authority, Fletcher, NC (Chair)
- Caroline Barnes, FBI Newark Division, Newark, NJ
- John McCarthy, Service Tec International, Reston, VA
- David E. Wilson, Port of Seattle, Seattle-Tacoma International Airport, Seattle, WA
- Martha A. Woolson, Alexandria, VA
- Abel Tapia, FAA Liaison
- Aneil Patel, Airports Council International–North America Liaison
- Christine Gerencher, TRB Liaison

Our Objective

Help airports establish and/or maintain effective airport cyber security programs based on best practices

- Increase awareness
- Provide training
- Offer resources

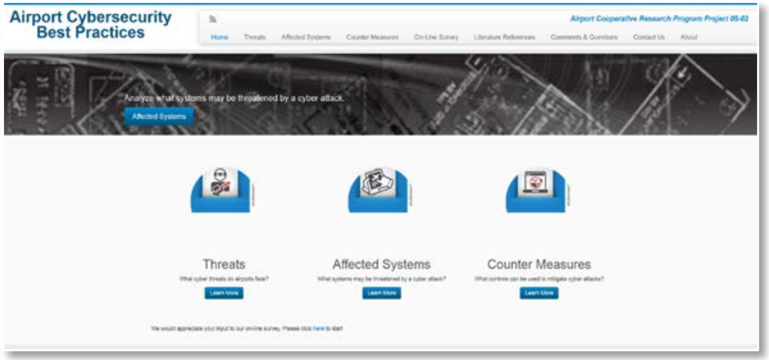
Our Approach

Secondary Research

- Literature search
- Other research initiatives
- Associations & committees

Primary Research

- Airports
- Other Industries: finance, heath care, utilities, etc.
- Information Sharing & Analysis Centers: MS-ISAC, A-ISAC
- Agencies: DHS, FBI, FAA



Analyze what systems may be threatened by a cyber attack.

Threats

What cyber threats do airports face?

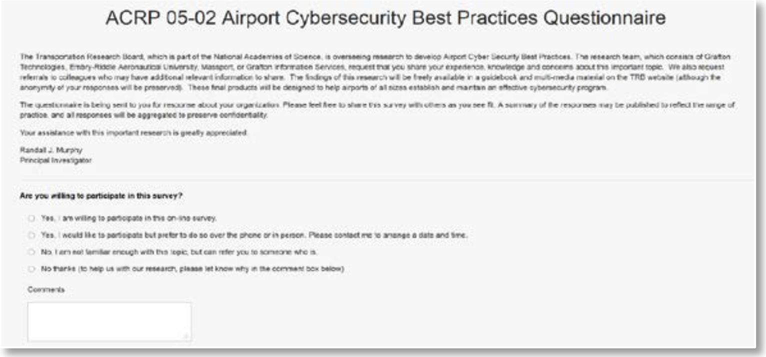
Affected Systems

What systems may be threatened by a cyber attack?

Counter Measures

What controls can be used to mitigate cyber attacks?

We would appreciate your input to our online survey. Please click here to start



ACRP 05-02 Airport Cybersecurity Best Practices Questionnaire

The Transportation Research Board, which is part of the National Academies of Science, is overseeing research to develop Airport Cyber Security Best Practices. The research team, which consists of Grafton Technologies, Embry-Riddle Aeronautical University, Massport, or Grafton Information Services, request that you share your experience, knowledge and concerns about this important topic. We also request referrals to colleagues who may have additional relevant information to share. The findings of this research will be freely available in a guidebook and multi-media material on the TRB website (although the anonymity of your responses will be preserved). These final products will be designed to help airports of all sizes establish and maintain an effective cybersecurity program.

The questionnaire is being sent to you for response about your organization. Please feel free to share this survey with others as you see fit. A summary of the responses may be published to reflect the range of practice, and all responses will be aggregated to preserve confidentiality.

Your assistance with this important research is greatly appreciated.

Randall J. Murphy
Principal Investigator

Are you willing to participate in this survey?

○ Yes, I am willing to participate in this on-line survey.
○ Yes, I would like to participate but prefer to do so over the phone or in person. Please contact me to arrange a date and time.
○ No, I am not familiar enough with this topic, but can refer you to someone who is.
○ No thanks (to help us with our research, please let know why in the comment box below)

Comments

Our Deliverables

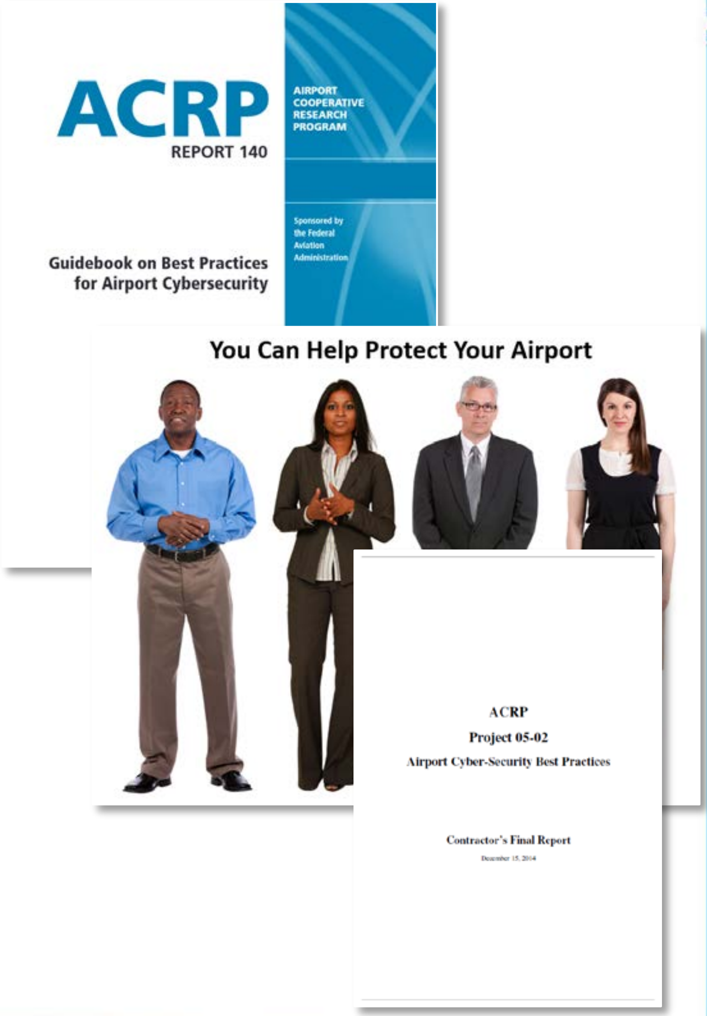
Guidance Document

- An approach to assessment
- Establishing and sustaining a cyber security program
- Detecting and Responding

Multi-Media Material

- Staff and employee training
- Material and resources

Contractor's Report



ACRP
REPORT 140

AIRPORT
COOPERATIVE
RESEARCH
PROGRAM

Sponsored by
the Federal
Aviation
Administration

Guidebook on Best Practices
for Airport Cybersecurity

You Can Help Protect Your Airport

ACRP
Project 05-02
Airport Cyber-Security Best Practices

Contractor's Final Report
December 15, 2014

ACRP
AIRPORT
COOPERATIVE
RESEARCH
PROGRAM

Key Findings

Apathy until attack is common

Attacks have and will likely continue

Concerns include

- Spear Phishing
- Industrial Control Systems
- Handling of Sensitive Information
- Bring Your Own Device
- Internal Threats

Sustainable cyber security program should be a goal

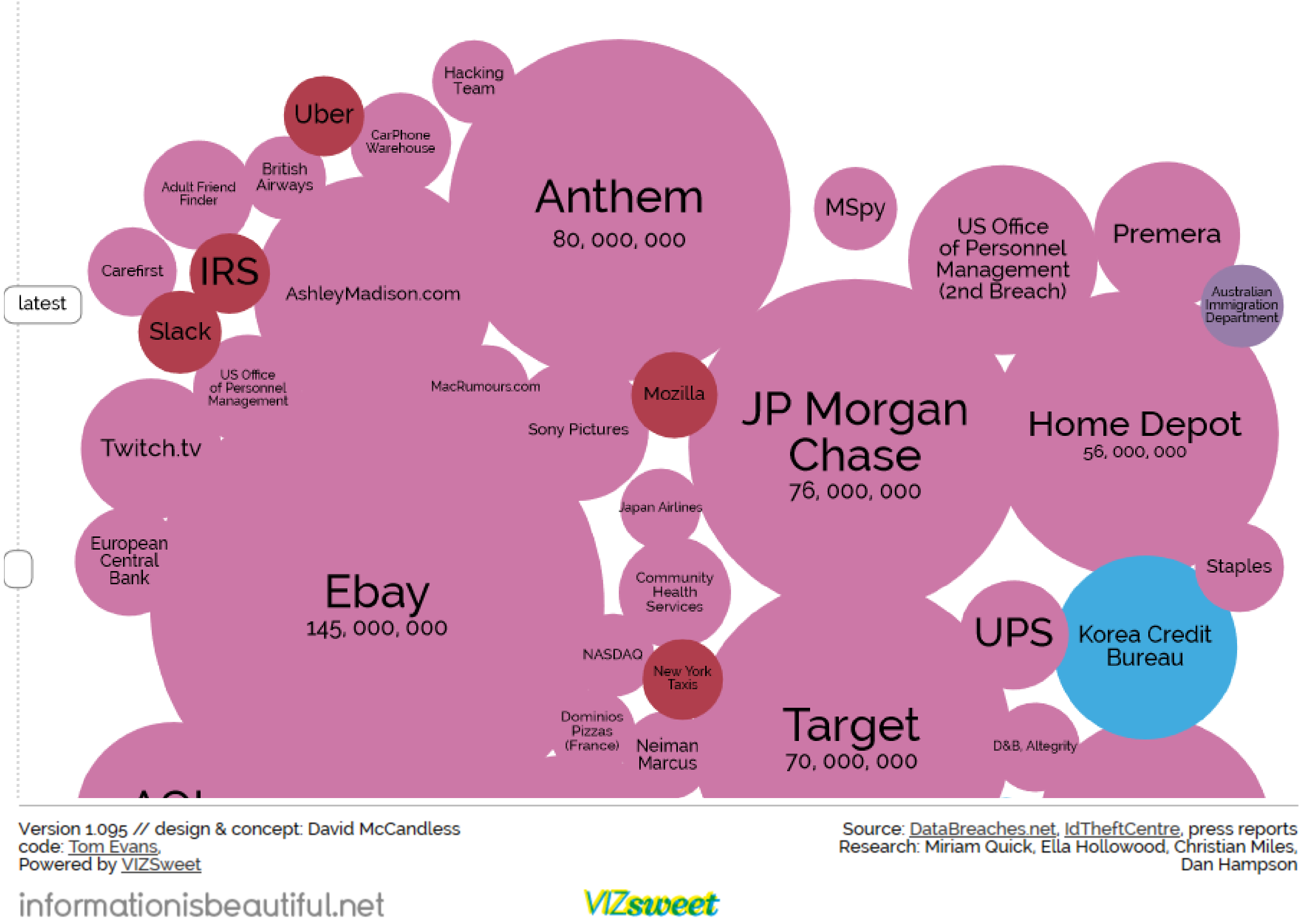
- Awareness
- Policy & Procedures
- Funding
- Communications & Training
- Response and recovery

Becoming a cost of doing business

We’re All Familiar With Attacks

ACRP

AIRPORT COOPERATIVE RESEARCH PROGRAM



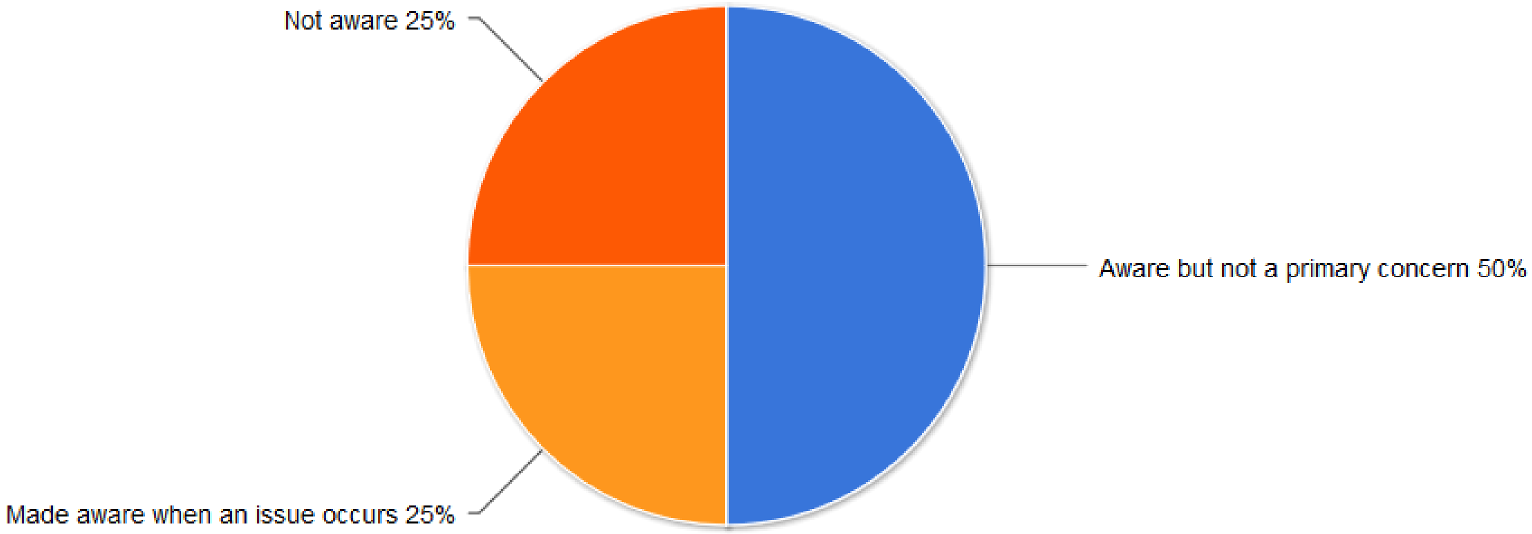
Version 1.095 // design & concept: David McCandless
code: Tom Evans,
Powered by VIZSweet

Source: DataBreaches.net, IdTheftCentre, press reports
Research: Miriam Quick, Ella Hollowood, Christian Miles, Dan Hampson

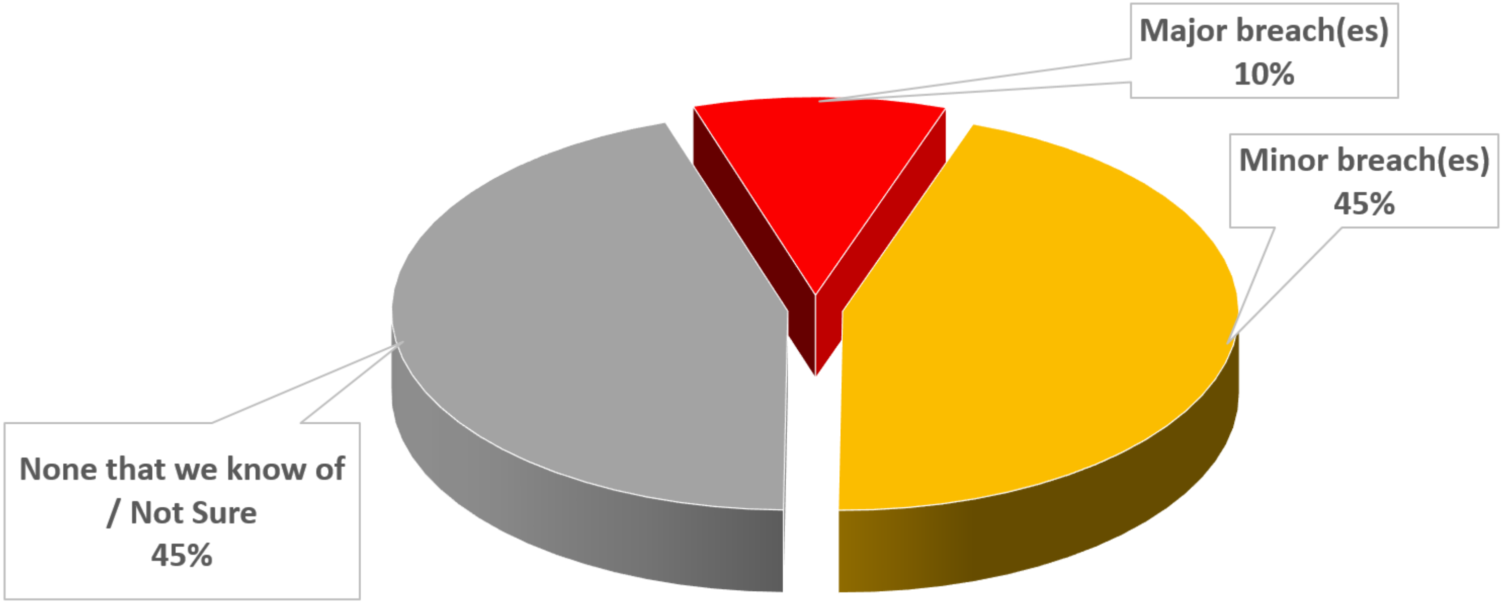
informationisbeautiful.net

VIZsweet

Apathy Until an Attack



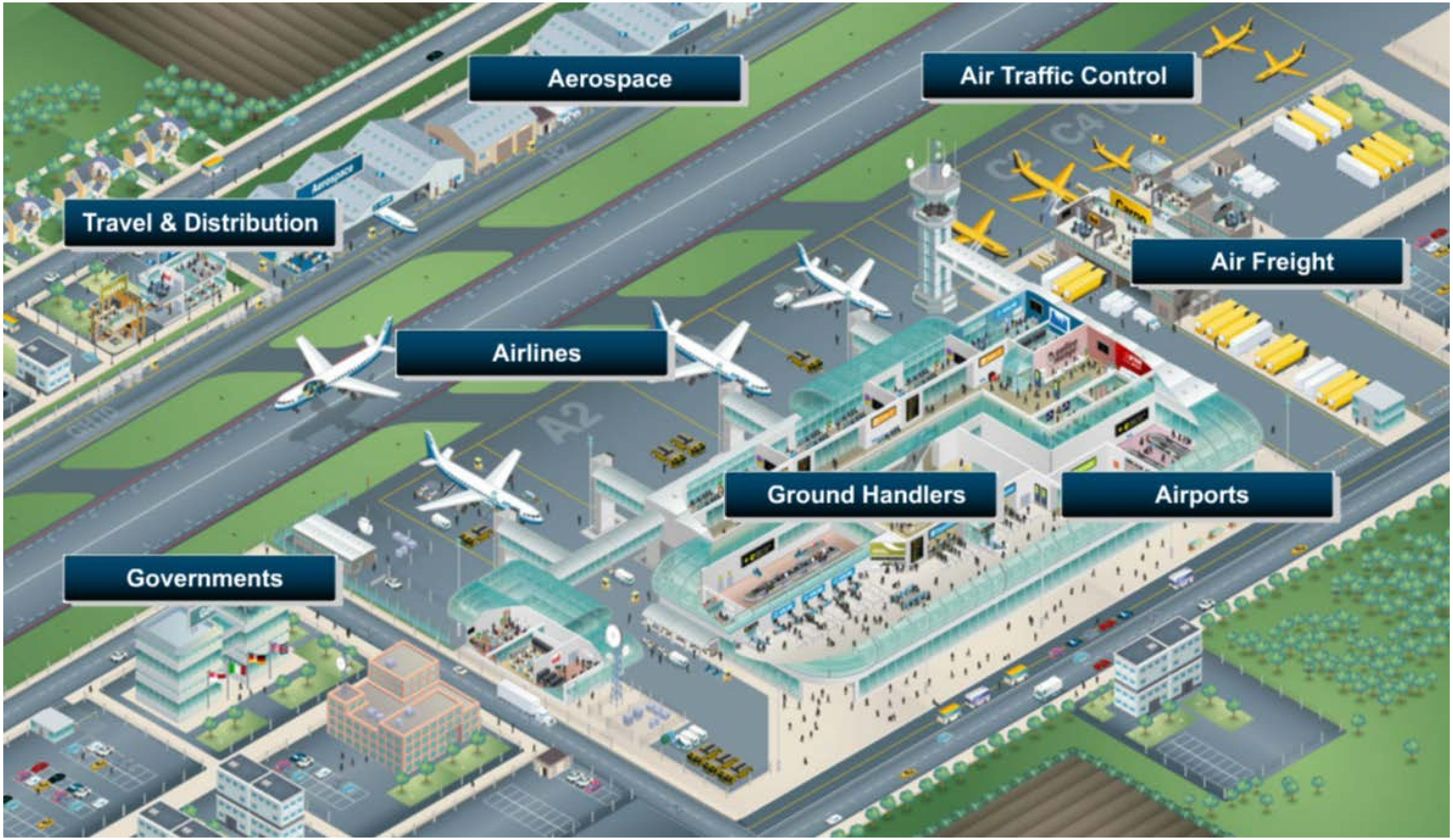
Airports Have Experienced Breaches



Some Examples

- Miami International Airport (MIA) has experienced almost 20,000 hack attempts per day before investing in training, education, and new hardware to protect itself from cyber-attacks (Computing, June 20, 2013)
- Los Angeles World Airports (LAX, ONT, VNY, and PMD) blocked almost 60,000 cases of internet misuse and 2.9 million hacking attempts in one year (Bob Cheong, Los Angeles World Airports)
- Istanbul's Ataturk International Airport (IST) had password control systems shut down by what is believed to have been a malware attack resulting in departure delays and extended waiting time for passengers (Security Affairs, July 28, 2013)
- An undisclosed major, non-U.S., international airport uncovered a variant of the Citadel Trojan malware that targeted Virtual private Network (VPN) credentials used by employees (Trusteer, August 12, 2012 and The Hacker News, August 16, 2012)
- The Dubai International Airport (DXB) had 50 email address and associated passwords stolen by a team of hackers from Portugal Cyber Army and the HighTech Brazil HackTeam (E Hacking News, April 19, 2013)
- The Catania–Fontanarossa Airport's (CTA) web-site was hacked and shut down for a few hours. A 22 year old suspect was believed to have illegally accessed and damaged data (The Hacker News, March 5, 2011)
- The Metropolitan Washington Airport Authority (MWAA) unintentionally published a document on its website containing Sensitive Security Information detailing the electronic security system at the Ronald Reagan Washington National Airport (DCA)

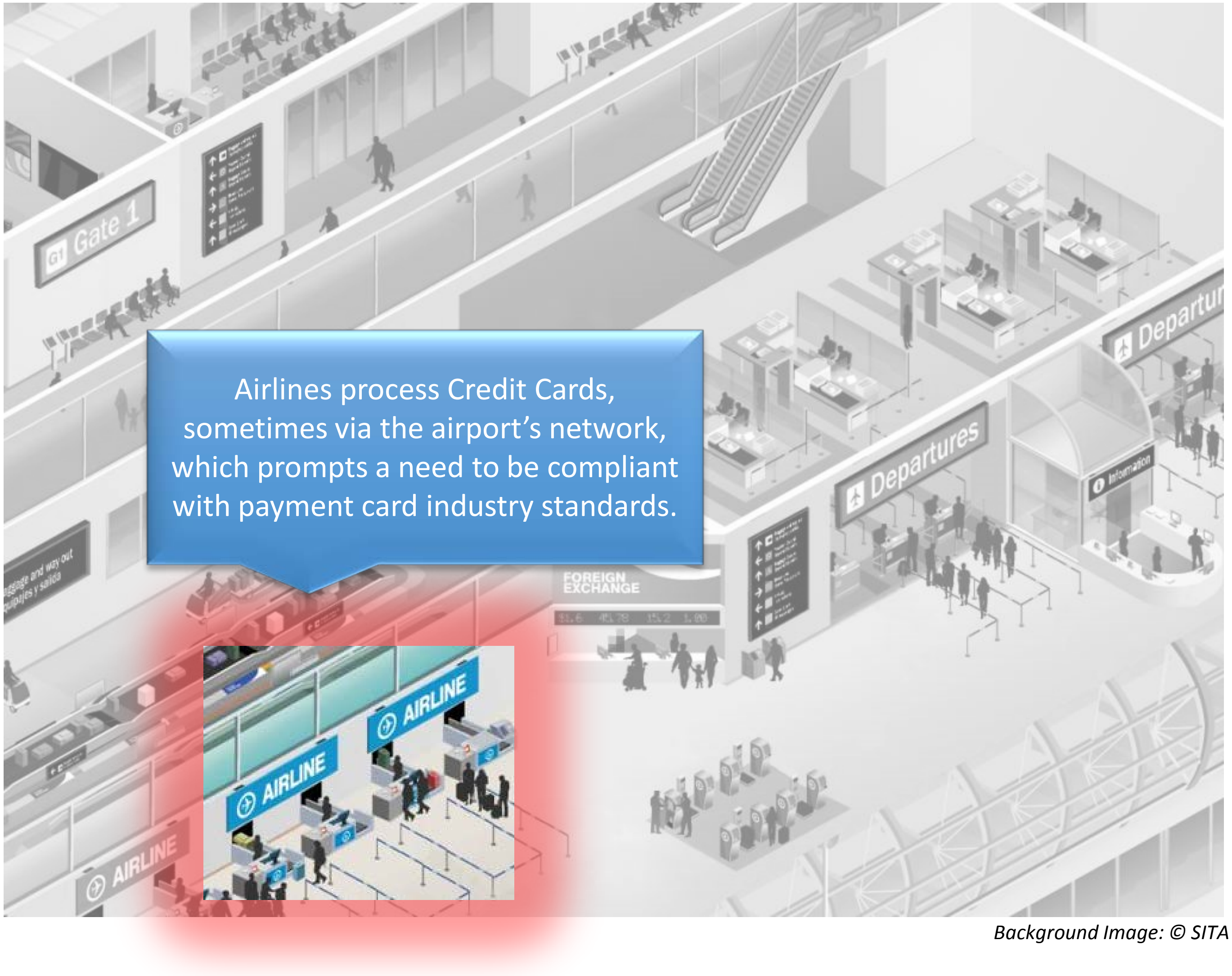
Where is Cyber Security Relevant at an Airport?



Background Image: © SITA

Pre-Security

Background Image: © SITA



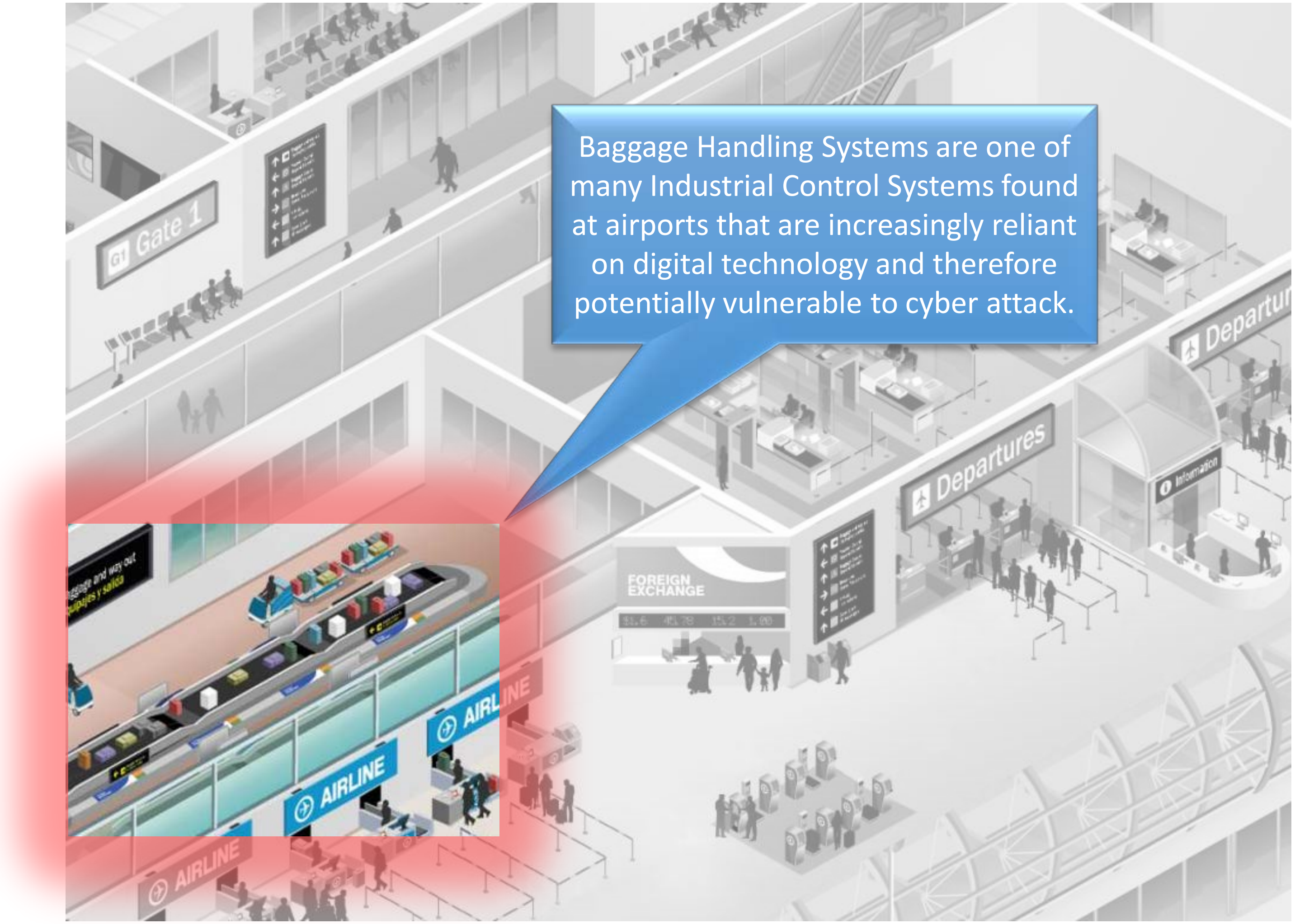
Airlines process Credit Cards, sometimes via the airport’s network, which prompts a need to be compliant with payment card industry standards.

Background Image: © SITA

G1 Gate 1
FOREIGN EXCHANGE
Departures
Departures
Information
AIRLINE
AIRLINE
AIRLINE

TSA, Customs, and Passport Control Operations are often outside of an airport's responsibility, but yet may introduce vulnerabilities that impact the airport.

Background Image: © SITA



Baggage Handling Systems are one of many Industrial Control Systems found at airports that are increasingly reliant on digital technology and therefore potentially vulnerable to cyber attack.

Background Image: © SITA

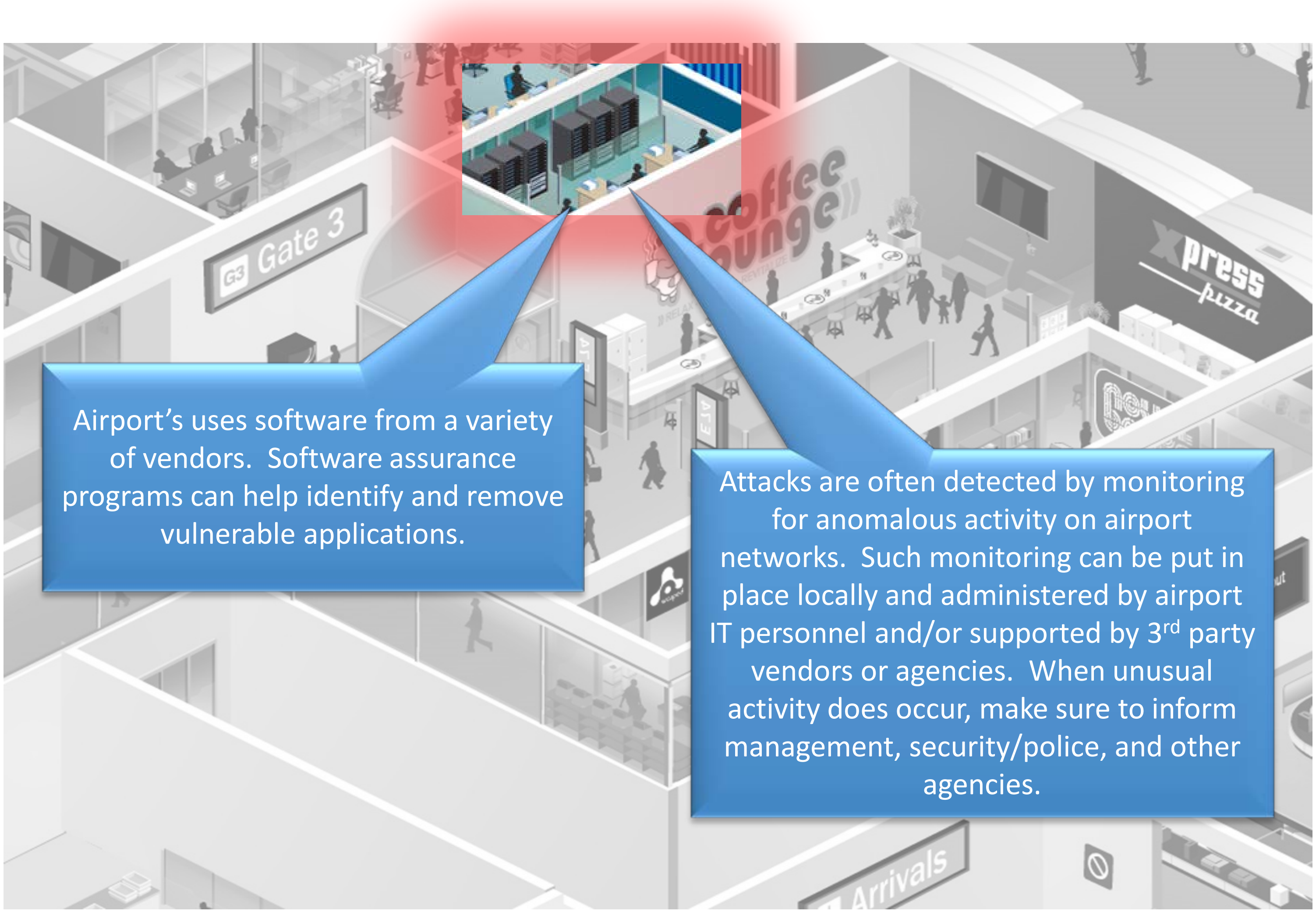
Post-Security

Background Image: © SITA

G3 Gate 3
coffee lounge
RELAX · RECLINE · REVITALIZE
xpress pizza
Baggage and way out
Equipajes y salida
Arrivals

Concessionaires and other tenants sometimes rely on an airport's IT infrastructure for point of sale devices and credit card processing. As with airlines, this prompts a need to be compliant with PCI standards.

Background Image: © SITA



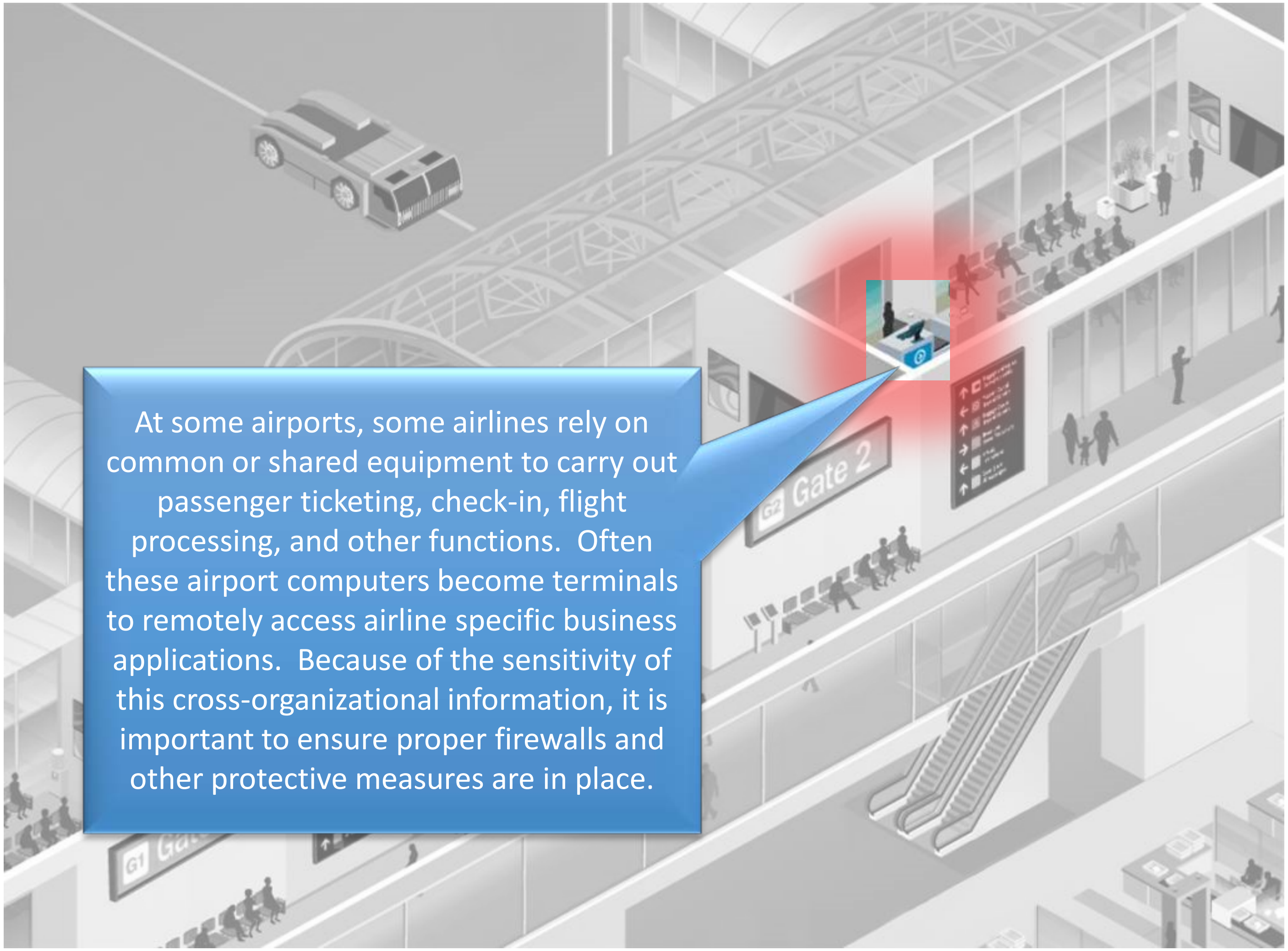
Airport’s uses software from a variety of vendors. Software assurance programs can help identify and remove vulnerable applications.

Attacks are often detected by monitoring for anomalous activity on airport networks. Such monitoring can be put in place locally and administered by airport IT personnel and/or supported by 3rd party vendors or agencies. When unusual activity does occur, make sure to inform management, security/police, and other agencies.

Background Image: © SITA

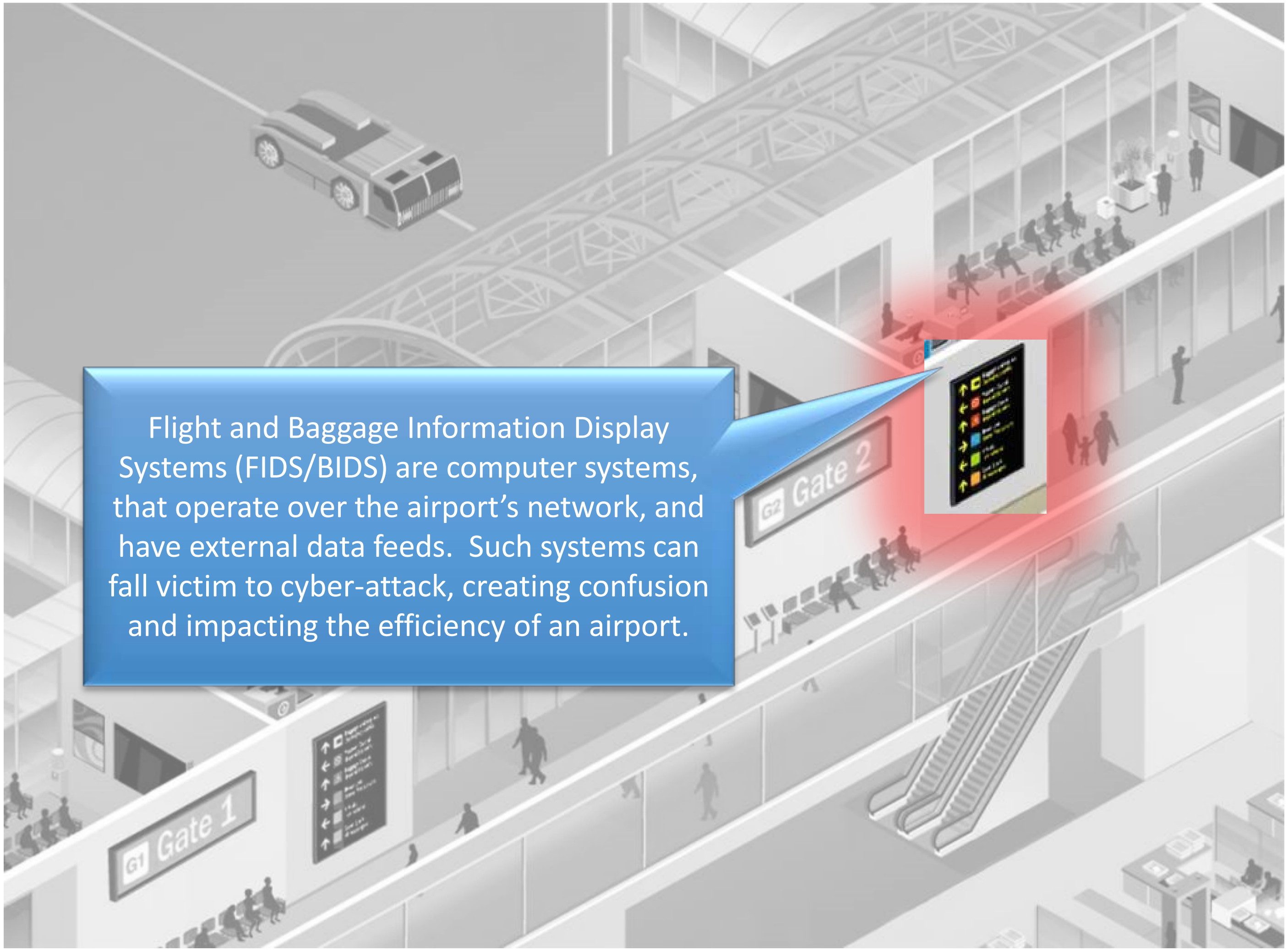
Airside

Background Image: © SITA



At some airports, some airlines rely on common or shared equipment to carry out passenger ticketing, check-in, flight processing, and other functions. Often these airport computers become terminals to remotely access airline specific business applications. Because of the sensitivity of this cross-organizational information, it is important to ensure proper firewalls and other protective measures are in place.

Background Image: © SITA



Flight and Baggage Information Display Systems (FIDS/BIDS) are computer systems, that operate over the airport's network, and have external data feeds. Such systems can fall victim to cyber-attack, creating confusion and impacting the efficiency of an airport.

Background Image: © SITA

At a growing number of airports, airline gate operations rely on airport wireless internet connectivity to access flight and corporate operational information. This exchange of potentially sensitive information should be adequately protected.

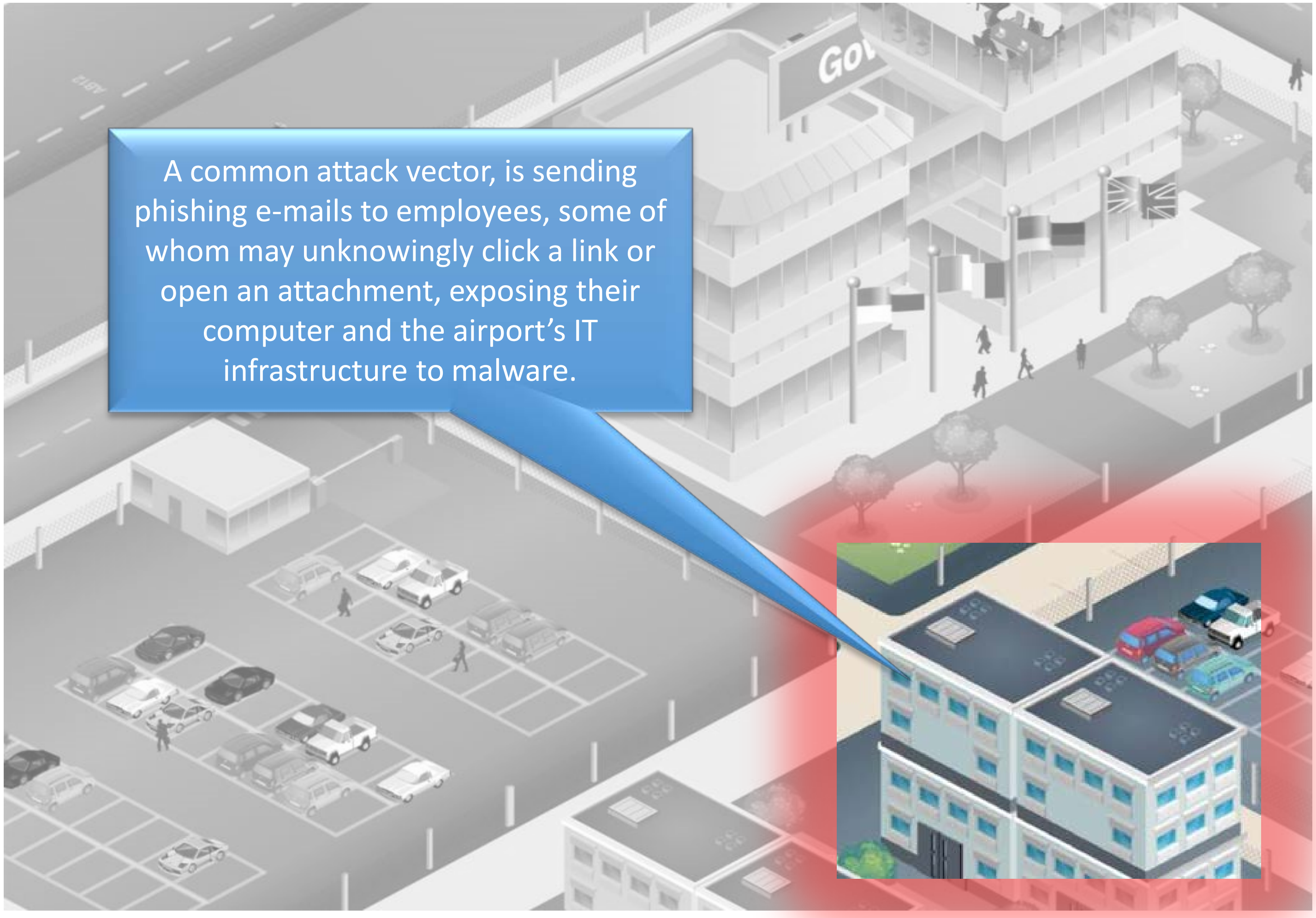
Background Image: © SITA

Outside the Terminal

Background Image: © SITA

Beyond the terminal environment, airport staff, consultants, and contractors exchange a great deal of digital information, some of it is sensitive and must be properly protected so as to not get into the wrong hands.

Background Image: © SITA

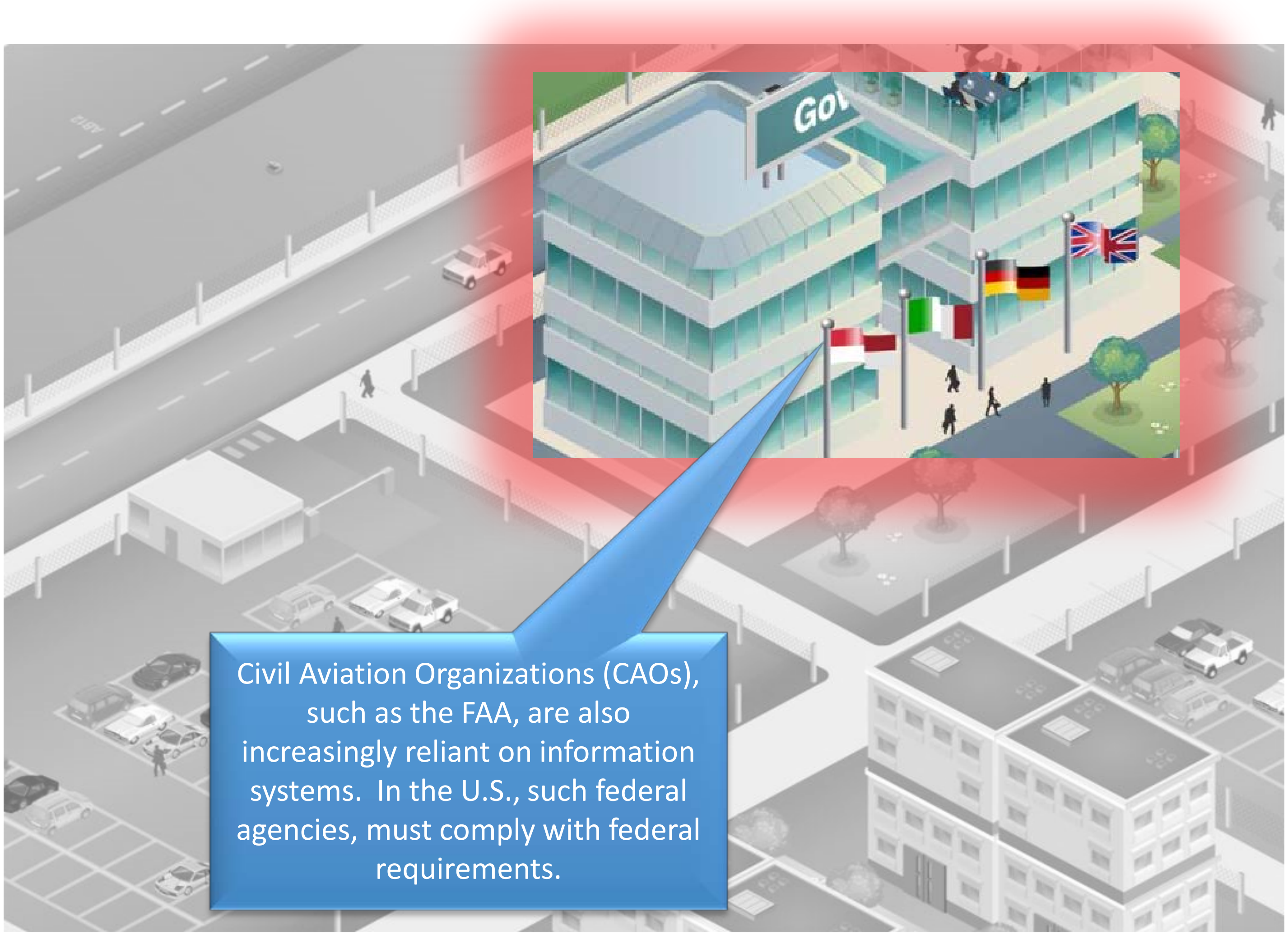


A common attack vector, is sending phishing e-mails to employees, some of whom may unknowingly click a link or open an attachment, exposing their computer and the airport's IT infrastructure to malware.

Background Image: © SITA

Parking is a significant source of revenue for many airports. Credit card transactions processed by the airport for parking fees require an airport to be PCI compliant.

Background Image: © SITA



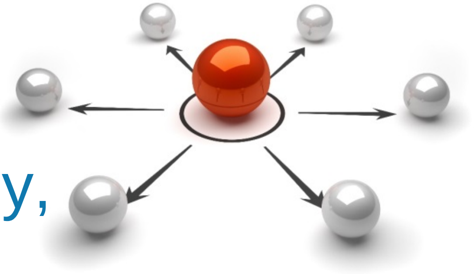
Civil Aviation Organizations (CAOs), such as the FAA, are also increasingly reliant on information systems. In the U.S., such federal agencies, must comply with federal requirements.

Background Image: © SITA

Threat Categories

- Confidentiality Breach
- Counterfeit Hardware
- Data Breach
- Delayed Technology Refresh
- Denial of Service
- Host Exploit
- Inadequate Monitoring of Proximity
- Events
- Ineffective Disposal
- Ineffective Testing
- Insider Threat
- insider threat/data breach
- Intentional Data Alteration
- Intentional Data Theft
- Internal Threat
- Labor Action
- Lack of Internal Control
- Malicious Code
- Organized Campaign
- Phishing
- Physical Exploit
- Social Engineering
- Supply Chain Integrity
- Third Party
- Unauthorized Access
- Unauthorized Host Access
- Unauthorized Network Access
- Unauthorized Physical Access
- Unauthorized Reconnaissance
- Unintended Data Compromise
- Unintended Data Leak
- Unpatched Hosts

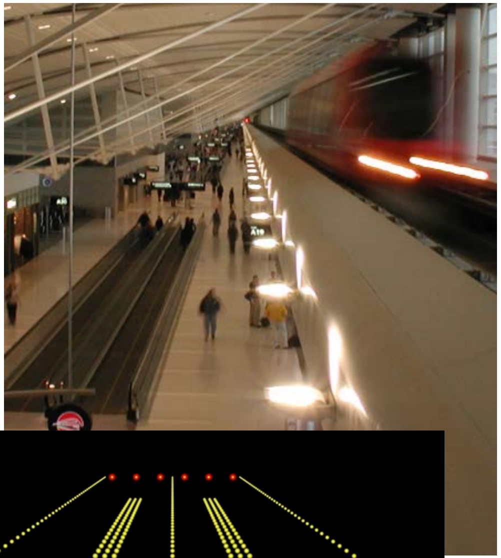
Integration Increases Risk

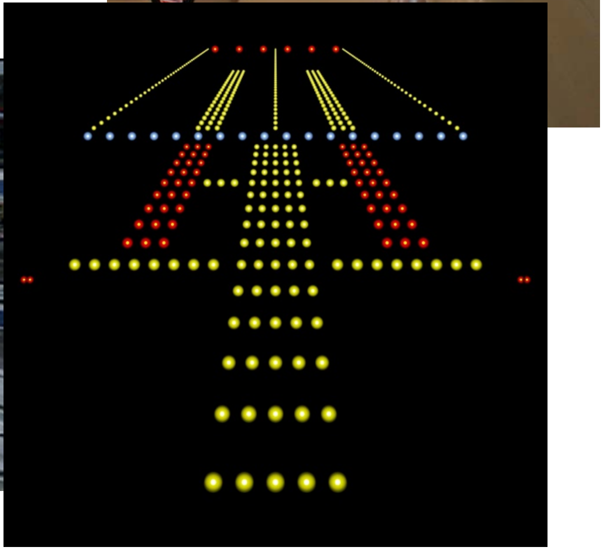


- Integration of systems increases operational efficiency, but highly integrated systems leave those systems vulnerable to security shortcomings of other systems
- Systems integration can fail when unique needs of the component systems are not addressed before design and deployment

Industrial Control Systems (ICS)

- Baggage Systems
- Building Automation Systems
- Heating Ventilation & Air Conditioning
- Airfield Lighting Systems
- Automobile Parking Systems
- Automated People Movers
- etc.

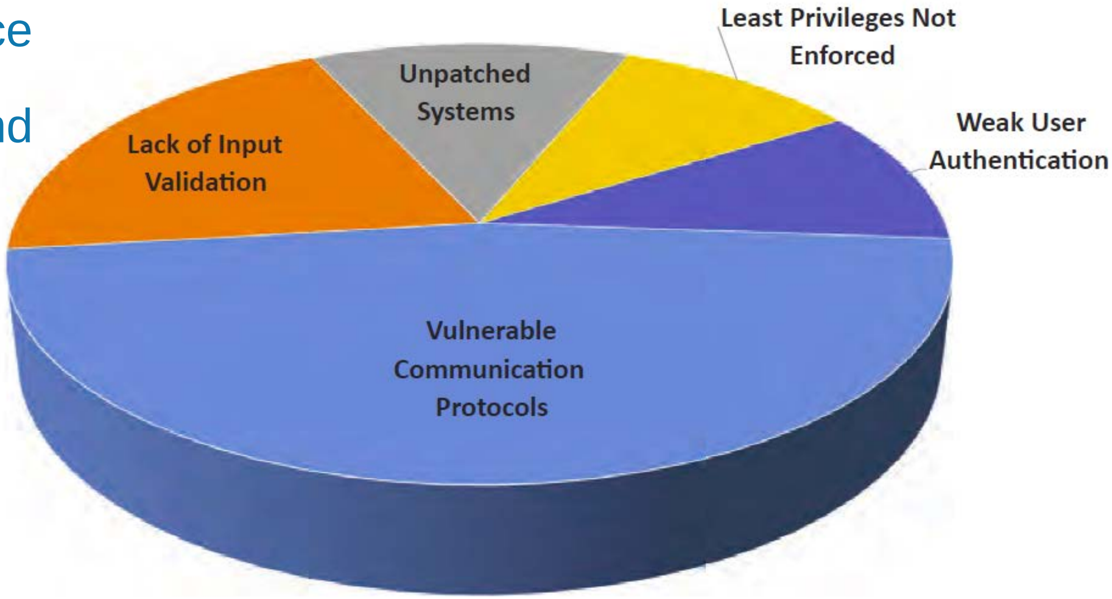




ACRP
AIRPORT COOPERATIVE RESEARCH PROGRAM

ICS Vectors of Attack

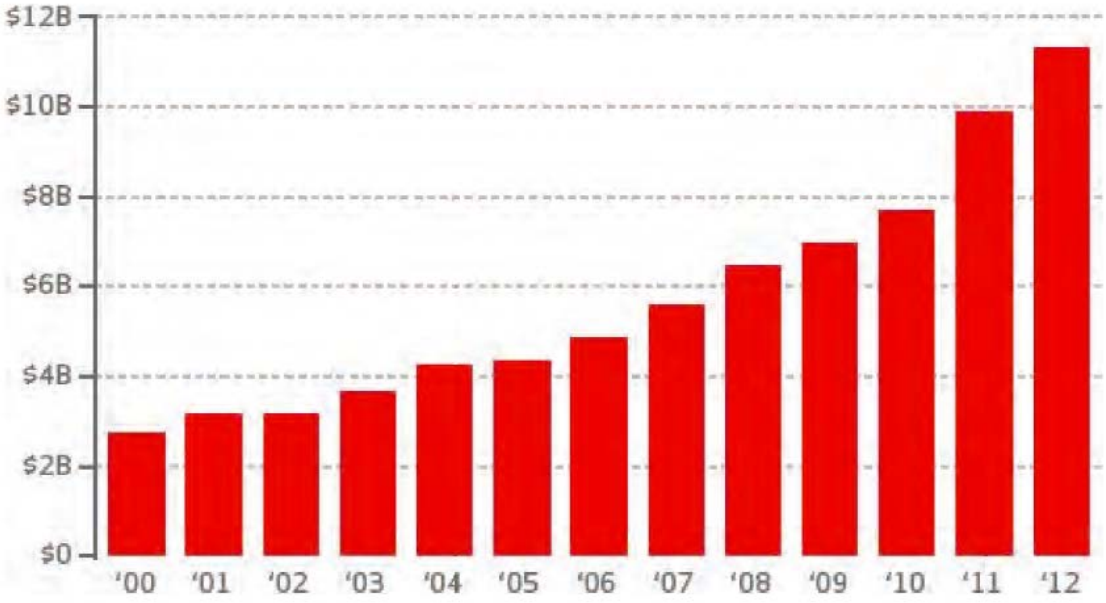
- Internet (hosted services or remote access)
- Sensor feeds and transmission
- Software maintenance monitoring, patches, and updates



Source: U.S. Department of Energy (2008).

Payment Card Industry (PCI)

- Airport process credit cards for parking & badging, and sometimes provide infrastructure for tenant sales
- Compliance with PCI standards may be mandatory
- Many feel it’s good practice regardless



Source: HSN Consultants, Inc. (2013).

BYOD

- Not all airport or organizations have an approach to BYOD to work
- Many users are not aware of good security practices to lock their portable devices and may unintentionally introduce a threat to Airport networks or may themselves be vulnerable to attacks
- Surveillance tools surreptitiously planted on a user’s handheld device are able to circumvent common mobile security

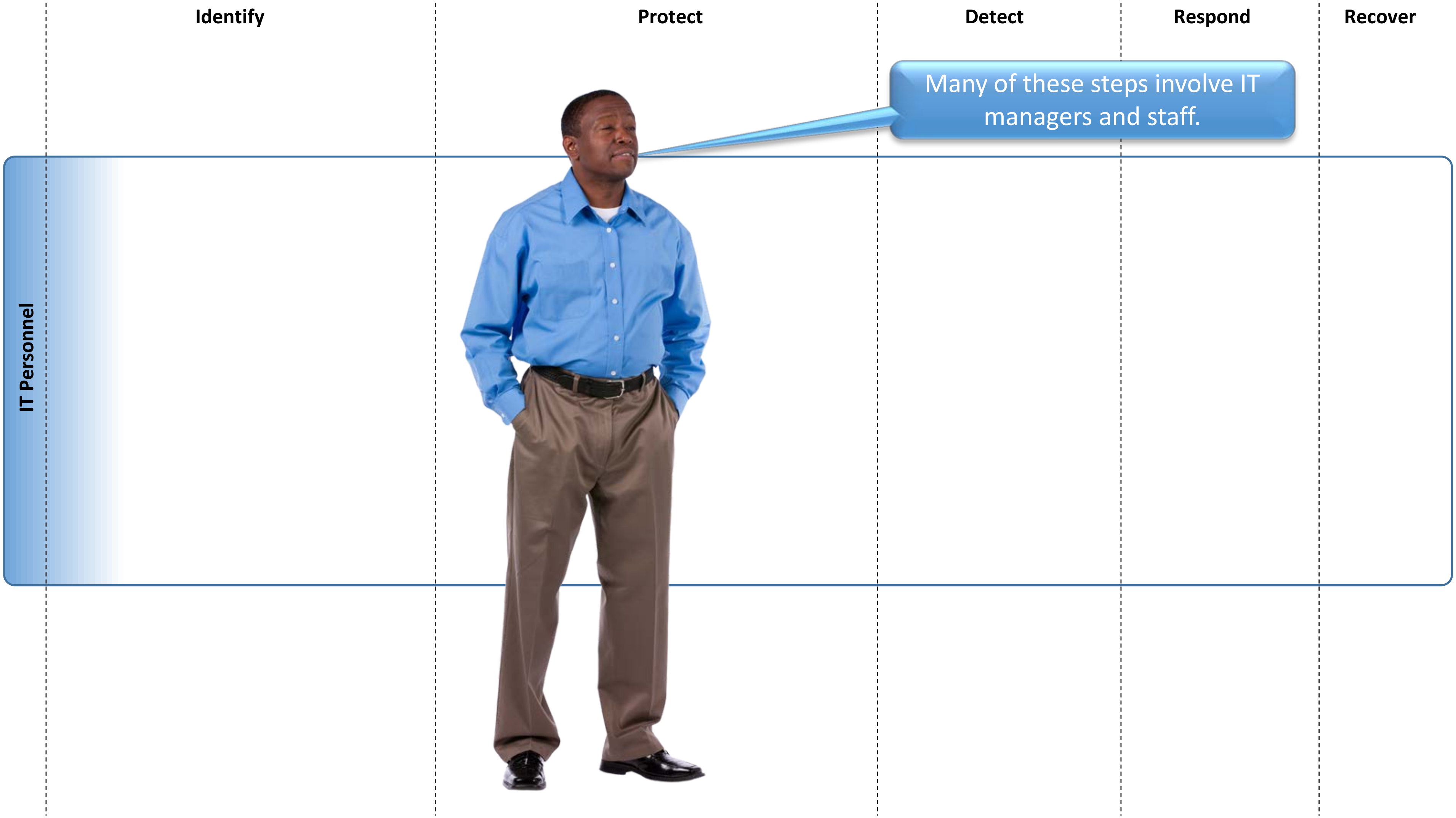
Human Factors

- Internet fraud losses are mostly attributable to exploit of human behavioral weakness
- 33% of respondents thus far report employees falling victim to social engineering
- Some feel that “cyber security countermeasures do not impose on employee privacy rights. They know that while on work, their data and computer usage are subject to scrutiny.”
- Half of the respondents block social media at work

Cyber Security Program

- 79% of respondents have a cyber security program; 46% felt that it provided adequate protection
- Airport cyber security programs (although not always called that) tend to fall under the Information Technology Department or, in a few instances, the Security Department
- Six respondents have individuals on staff that have the title of Cyber Security Manager who report to a CTO or CIO
- Optimal Programs Consist of:
  - Technology Centric unit
  - Risk management unit with strategic view
  - Day to day operational unit
- 47% outsource cybersecurity functions, 80% use third parties for vulnerability testing
- A holistic security risk management methodology is scalable and can cover a single area to the entire airport infrastructure

Identify	Protect	Detect	Respond	Recover



Identify

Protect

Detect

Respond

Recover

IT Personnel

Many of these steps involve IT managers and staff.

Identify

Protect

Detect

Respond

Recover

IT Personnel

But we’re not alone!

Identify

Protect

Detect

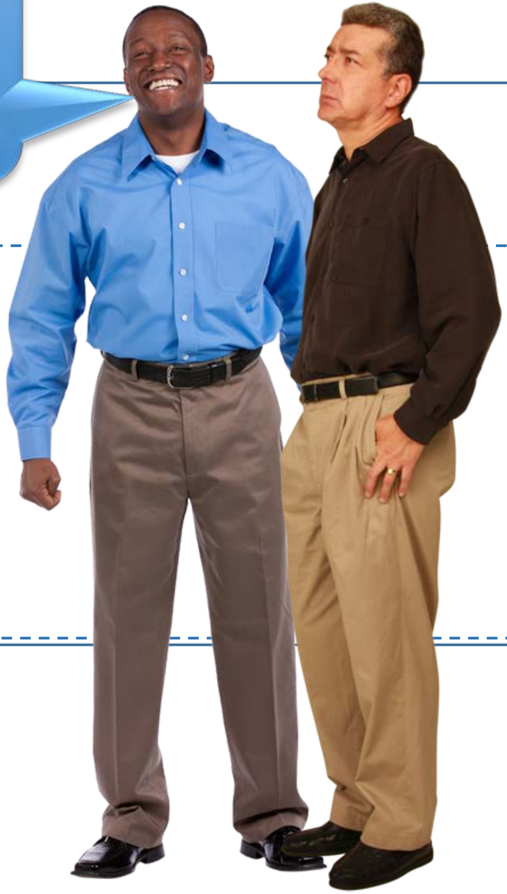
Respond

Recover

IT Personnel

A growing number of consultants, vendors, non-government agencies, and other 3rd party providers are available to help

Potential Role for Service Providers



Identify | Protect | Detect | Respond | Recover

Management

Airport Executive Managers should be supportive, but can also play an active role in some key areas.

Identify

Protect

Detect

Respond

Recover

There are a lot of things all airport staff members can do.

Staff

Identify

Protect

Detect

Respond

Recover

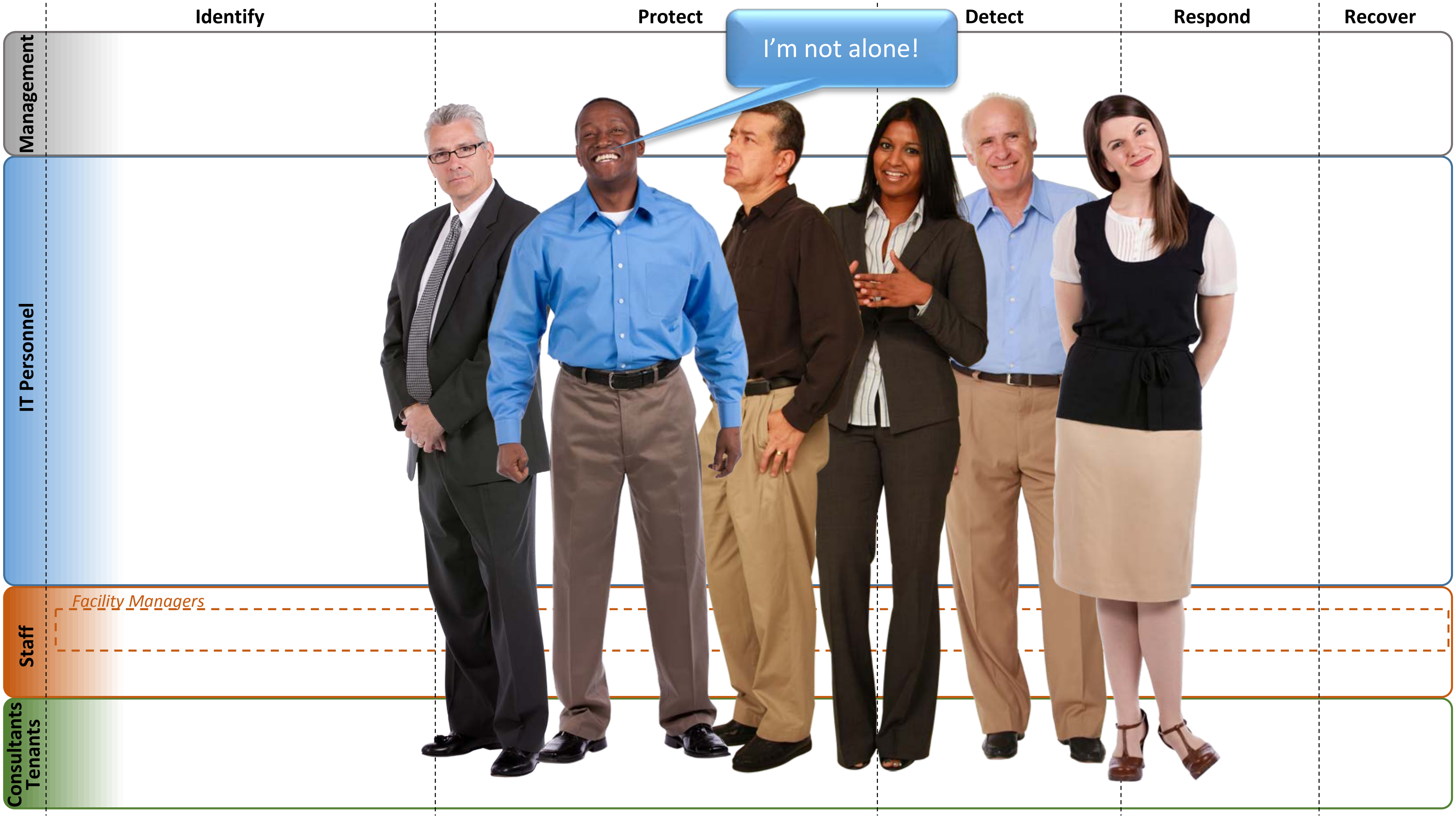
Facility Managers should also work closely with IT so that the Industrial Control Systems they are in charge of are properly protected from cyber attack.

Staff

Facility Managers

	Identify	Protect	Detect	Respond	Recover
Consultants Tenants					

Consultants and Tenants also play a role at protecting the airport(s) they work for or at against cyber attacks.



Identify

Protect

Detect

Respond

Recover

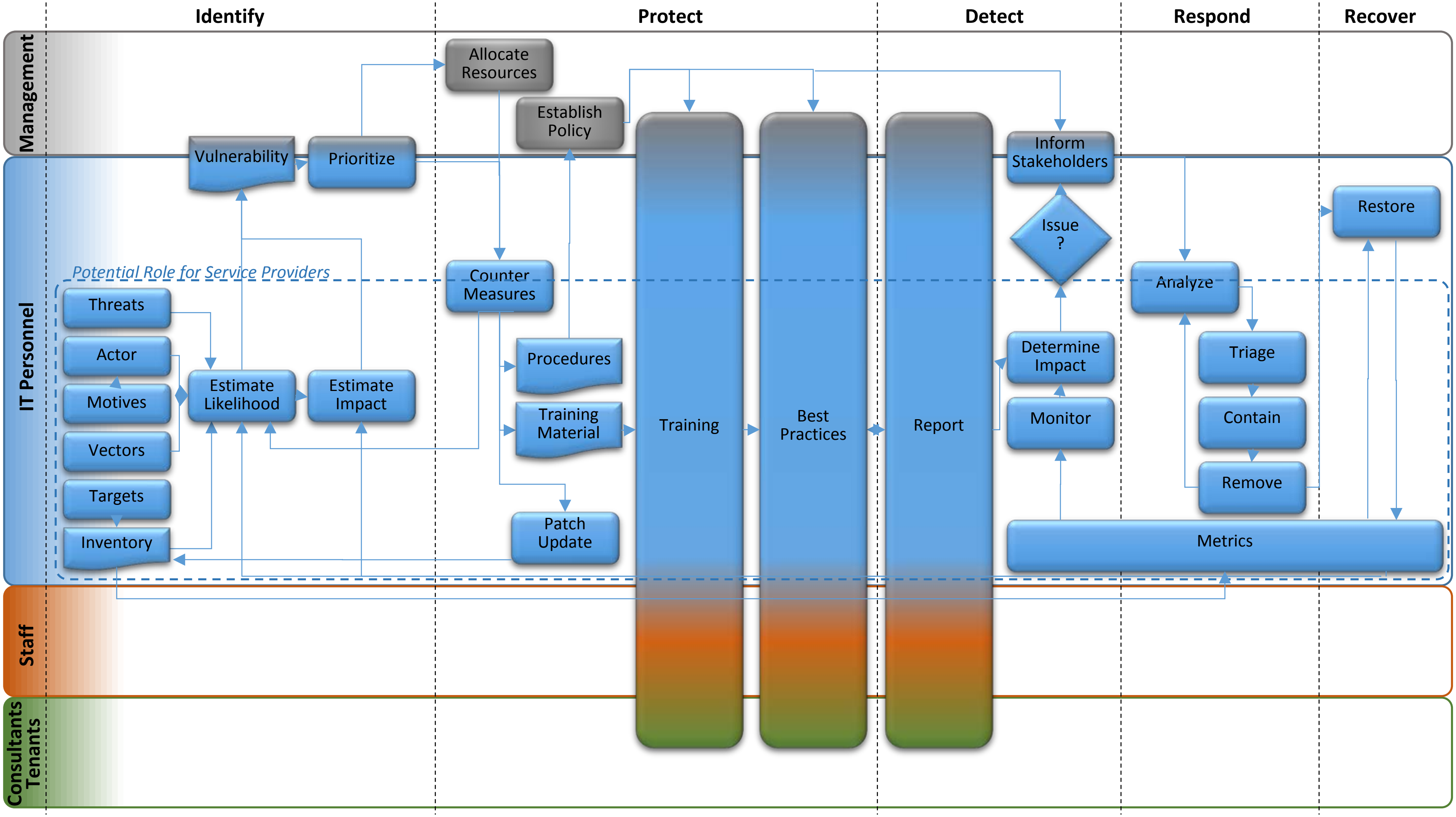
Management

IT Personnel

Staff

Facility Managers

Consultants
Tenants


Identify
Protect
Detect
Respond
Recover
Management
IT Personnel
Staff
Consultants
Tenants
Allocate Resources
Establish Policy
Vulnerability
Prioritize
Inform Stakeholders
Restore
Issue ?
Potential Role for Service Providers
Counter Measures
Analyze
Threats
Actor
Motives
Vectors
Targets
Inventory
Estimate Likelihood
Estimate Impact
Procedures
Training Material
Patch Update
Training
Best Practices
Report
Determine Impact
Monitor
Triage
Contain
Remove
Metrics

Assessing Vulnerabilities

- Most feel that their cyber security readiness is either good or excellent
- Vulnerability Testing in Place:
  - 90% network
  - 63% physical
  - 53% software applications
  - 36% social engineering
- Some feel that risk assessments can often be inefficient and costly

ACRP

AIRPORT
COOPERATIVE
RESEARCH
PROGRAM

Addressing Vulnerabilities

Management

- Planning
- Program Management
- Risk Assessment
- Security Assessment & Authorization
- System & Services Acquisition

Technical

- Access Control
- Audit & Accountability
- Identification & Authentication
- System & Communications Protection

Operational

- Awareness & Training
- Configuration
- Contingency Planning
- Incident Response
- Maintenance
- Media Protection
- Personnel Security
- Physical & Environmental Protection
- System & Information Integrity

Policies & Procedures

- Most airports have written policies governing the use of airport computers, although they may not always enforce these policies by implementing restrictions on the network, PCs, or user accounts.
- Airports generally have employee policies and procedures, as well as IT policies and procedures. The cybersecurity content in these documents can be enhanced.
- A centralized inventory of assets that includes device identities, asset information, and digital footprint doesn't typically exist at airports.

Computer and Data Use

Sensitive Security Information

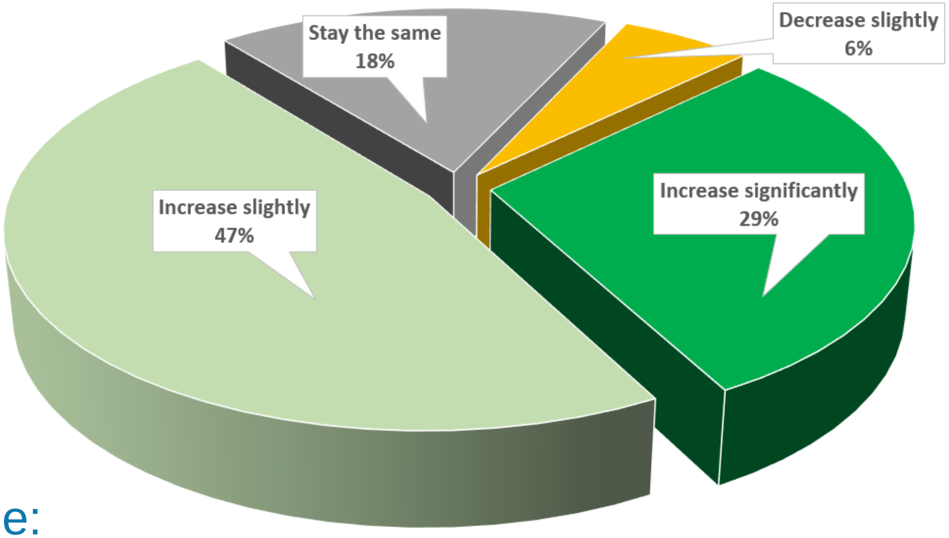
Bring Your Own Devices

Response & Recovery

- Continuity of Operations and Disaster Response Plans are new and emerging
- Airports need incidence response procedures, including resources to contact when a problem occurs
- Pre-existing knowledge of and relationships with contacts is important
- Cyber awareness of local law enforcement and airport security helps

Funding

- Airports dedicate relatively little to cyber security
- Cyber security spending is on the rise



- Motivators include:
  - Results of threat assessments and vulnerability tests
  - Preventing service interruption
  - Prevent property damage
  - Compliance with regulations

Training

- Education and training of airport employees in cyber security practices can protect the airport from cyber attacks
- Most respondents have in-house cyber security training programs, which is delivered throughout the organization.
- Half of the respondents said that their cyber security training budget would stay the same. A third said it would increase.
- Rapid changes within technology, software developments, and the evolving sophistication of attack methods is a key challenge faced by security and IT administrators

Roles & Responsibilities

IT Professionals Should

- ✓ Develop and periodically update an inventory of systems
- ✓ Conduct vulnerability assessments of those systems
- ✓ Implement counter measures to eliminate or reduce vulnerabilities
- ✓ Monitor for anomalous activity
- ✓ Report attacks and other suspicious activity
- ✓ Implement tested recovery plans
- ✓ Train staff, consultants and tenants

Roles & Responsibilities

Airport Staff Should

- ✓ Be aware of cyber security threats and your role in protecting against them
- ✓ Participate in periodic training
- ✓ Carry out best practices
  - Use and protect strong passwords
  - Beware of phishing emails
  - Identify and protect sensitive data
  - Adhere to policy and procedures
- ✓ Report issues or concerns to IT

Roles & Responsibilities

Senior Management Should

- ✓ Be aware of cyber security threats and how they can impact their airport
- ✓ Support the development of a cyber security program
- ✓ Set policy that enforces best practices
- ✓ Follow the same procedures as their staff

Airport Staff Should

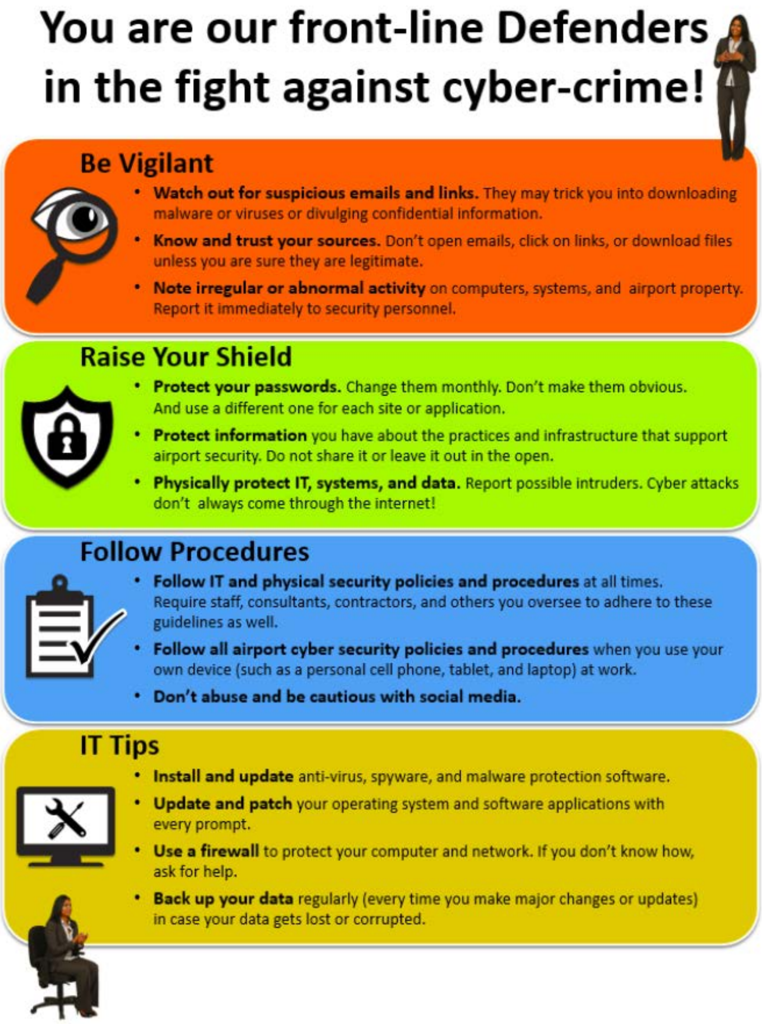
- ✓ Be aware of cyber security threats and your role in protecting against them
- ✓ Participate in periodic training
- ✓ Carry out best practices
  - Use and protect strong passwords
  - Beware of phishing emails
  - Identify and protect sensitive data
  - Adhere to policy and procedures
- ✓ Report issues or concerns to IT

Roles & Responsibilities

Consultants Should

- ✓ Be aware of cyber security threats and your role in protecting against them
- ✓ Ensure project teams are aware of their client’s policy and procedures
- ✓ Carry out best practices
  - Use and protect strong passwords as their corporate policy requires
  - Beware of phishing emails
  - Identify and protect sensitive data
- ✓ Report issues or concerns to their management

Daily Reminders



You are our front-line Defenders in the fight against cyber-crime!

Be Vigilant

- **Watch out for suspicious emails and links.** They may trick you into downloading malware or viruses or divulging confidential information.
- **Know and trust your sources.** Don't open emails, click on links, or download files unless you are sure they are legitimate.
- **Note irregular or abnormal activity** on computers, systems, and airport property. Report it immediately to security personnel.

Raise Your Shield

- **Protect your passwords.** Change them monthly. Don't make them obvious. And use a different one for each site or application.
- **Protect information** you have about the practices and infrastructure that support airport security. Do not share it or leave it out in the open.
- **Physically protect IT, systems, and data.** Report possible intruders. Cyber attacks don't always come through the internet!

Follow Procedures

- **Follow IT and physical security policies and procedures** at all times. Require staff, consultants, contractors, and others you oversee to adhere to these guidelines as well.
- **Follow all airport cyber security policies and procedures** when you use your own device (such as a personal cell phone, tablet, and laptop) at work.
- **Don't abuse and be cautious with social media.**

IT Tips

- **Install and update** anti-virus, spyware, and malware protection software.
- **Update and patch** your operating system and software applications with every prompt.
- **Use a firewall** to protect your computer and network. If you don't know how, ask for help.
- **Back up your data** regularly (every time you make major changes or updates) in case your data gets lost or corrupted.

Training Providers & Other Resources

Training Providers

- PCI Essentials
  www.pci-essentials.com
- Texas A&M Engineering Extension Service (TEEX)
  http://teex.com/nerrtc/ (click on cybersecurity)
- Vendors and Consultants

Resources

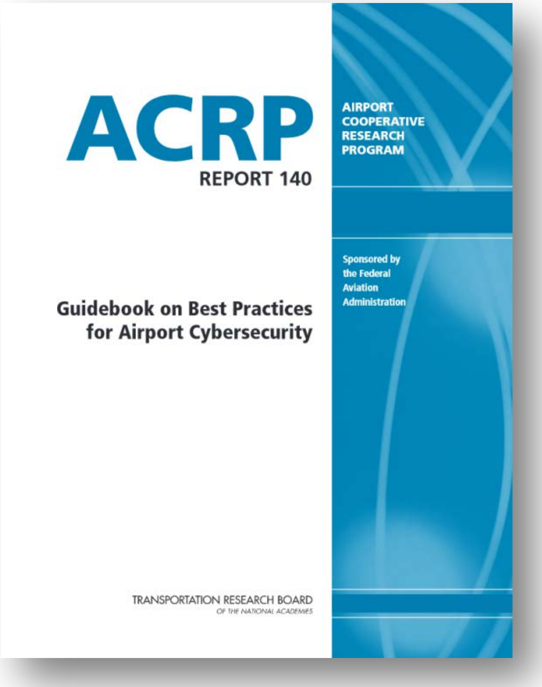
- Our project's web-site
  www.airportcyber.com
- National Institute of Standards & Technology
  www.nist.gov
- SANS Reading Room
  http://www.sans.org/reading-room/

Keeping Up To Date

- ISACs
- Service Providers
- Associations (e.g. ACI-NA’s BIT, AAAE, ACC)
- Agencies (e.g. DHS and FBI)
- Peer to peer communication

AVIATION ISAC

For additional information



ACRP
REPORT 140

AIRPORT
COOPERATIVE
RESEARCH
PROGRAM

Sponsored by
the Federal
Aviation
Administration

Guidebook on Best Practices
for Airport Cybersecurity

TRANSPORTATION RESEARCH BOARD
OF THE NATIONAL ACADEMIES

ACRP Report 140

A Guidebook on Best Practices for Airport Cybersecurity

http://www.trb.org/main/blurbs/172854.aspx

Randy Murphy

RMurphy@GraftonTech.com

ACRP Report 127: A Guidebook for Mitigating Disruptive WiFi Interference at Airports

Michael Carroll,
System Planning Corporation
Stephen Berger,
TEM Consulting, LP

ACRP
AIRPORT
COOPERATIVE
RESEARCH
PROGRAM

Michael Carroll
Principal Investigator

- Center Director, Wireless Communications and Analysis, System Planning Corporation (SPC*)
- Career USAF Communications-Electronics Officer

Stephen Berger
Lead Engineer

- President, TEM Consulting
- Chair:
  - ANSI ASC C63 SC6 – Spectrum Management
  - ANSI C63.27 – Wireless Coexistence Testing
  - IEEE 1900.2 – Wireless Coexistence Analysis

- * SPC is now SPC-Federal, LLC, a subsidiary of ECS-Federal, LLC

ACRP Report 127 Oversight Panel

- *John Newsome*, Greater Orlando Aviation Authority, FL. (Chair)
- *Pamela E. Bell*, Ross & Baruzzini, Inc., Bellevue, WA
- *John A. Buckner*, Salt Lake City Department of Airports, Salt Lake City, UT
- *Timothy M. Mitchell*, Boeing, Seattle, WA
- *Jeffrey Rae*, United Airlines, Chicago, IL
- *Dawoud Stevenson*, Savannah Airport, Savannah GA
- *Kiem Hoang*, FAA Liaison
- *Alvin Logan*, FAA Liaison
- *Aniel Patel*, Airports Council International-North America Liaison

ACRP

AIRPORT
COOPERATIVE
RESEARCH
PROGRAM

Problem – Assuring Reliability of Wireless Services at Airports

- How to ensure reliability and acceptable performance of wireless services in the face of growing spectral congestion
- Potential problems**:**
  - Radio frequency (RF) interference
  - Equipment interoperability
  - Network congestion
  - Poor coverage
  - Reliability, priority, and security (for airport operations)
- Environment:
  - There are a few bands that are congregating points for a wide variety of services
  - Some of the most congested bands are open access and under FCC rules *airports cannot regulate use of these bands or prohibit travelers and vendors from using their own equipment*

ACRP Report 127:
A Guidebook for Mitigating Disruptive WiFi Interference at Airports

- Quantifies extent and magnitude of interference problems
- Identifies best technical and business practices to provide accessible service with adaptable bandwidth for all stakeholders
- Recommends a cooperative approach via communication and collaboration among parties to maximize benefits
- References a design adaptable to all airport environments (small, medium, large) to meet needs of all stakeholders
- Provides techniques for identifying and resolving interference outside reference design
- Enables a strategic vision that addresses potential impacts due to increasing demand, evolving technologies, and new requirements
- Addresses total cost of ownership and return on investment
- Published 2015

ACRP

AIRPORT
COOPERATIVE
RESEARCH
PROGRAM

Research Approach

- Defined the problem:
  - What is RF interference and its impact on WiFi services
  - Understanding that WiFi services are transitioning from being a high-end consumer amenity used by relatively few passengers to services now expected to be available for all passengers as well as businesses and airport operations
- System approach**:**
  - Developed an RF interference primer, quantified the RF interference problem, and identified techniques to mitigate RF interference
  - Queried airports regarding their WiFi experience, capacity, and performance
    - Developed survey for 18 airports
    - Visited nine airports
- Provided a WiFi strategy that supports communications and collaboration among all stakeholders and addresses increased demand, evolving technologies, available WiFi tools, and new requirements

Research Results

- A few bands, particularly those used by WiFi, are heavily used and increasingly congested.
- Data traffic and wireless applications are growing, resulting in increased congestion in the future.
- The importance of WiFi and wireless services in general has always been important to airports but is becoming even more important and important to a growing number of areas of airport operations.
- Airports generally have sub-contracted wireless network management and as a result have limited expertise or experience with network management.
- Airport Growth trends in spectral congestion needs to be monitored so that management plans can anticipate rather than respond to growing congestion.

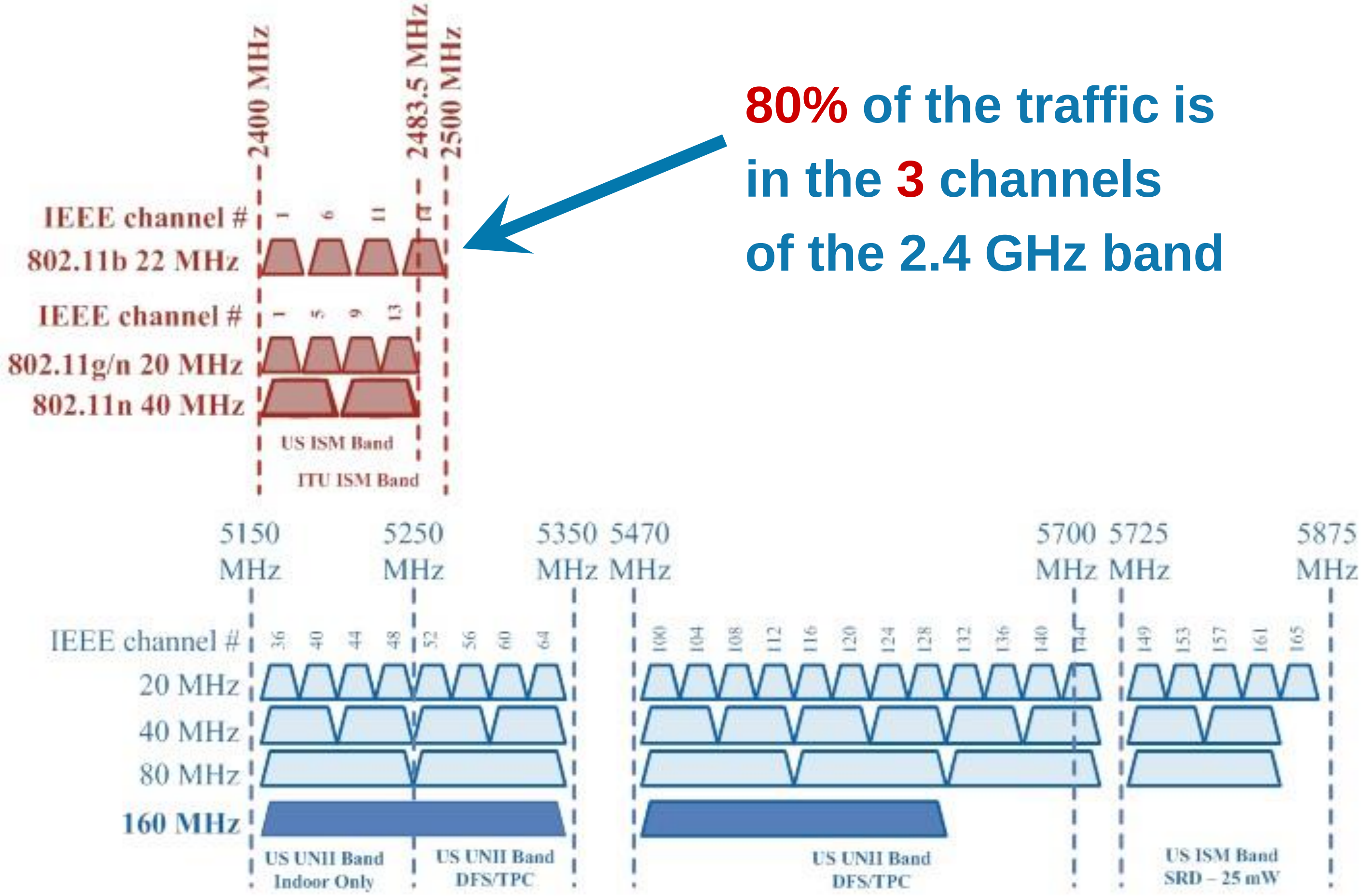
Results – Understanding RF Interference

- RF interference versus daily morning and evening commute - limited roads and rail choices creates recurring congestion and regular accidents.
- Spectrum use is similar the morning commute: spectrum users go to the same few bands and even the same few channels in those bands.
  - There are good reasons, but it creates spectral congestions and interference
  - Congestion has to be managed, it is difficult to prevent (think of HOV lanes vice telling people they cannot go to work in the morning)
- A wireless network is not a wired network without wires, it has its own dynamics and characteristics. Managing wireless networks is its own specialty

Results – Understanding RF Interference

- RF interference associated with “unlicensed” WiFi spectrum – involves dealing with several different issues
- Case study results:
  - Poor understanding of the range and variation of indoor RF environments
  - Dominate source of WiFi interference is from other WiFi devices.
  - Strong correlation between band crowding and interference
  - Co-location of WiFi and cellular network antennas
  - Technology changes – older systems inability to properly interface with newer systems
  - Customer complaints were major metric to determine performance quality
- Proper network design and management can eliminate potential RF interference
- Stakeholder cooperation can improve planning, performance, and reduce interference

Spectrum Allocation
2.4 and 5 GHz WiFi Channels



80% of the traffic is
in the **3** channels
of the 2.4 GHz band

Packet Retransmission Rates

Date	Location	2.4 GHz Band - Retransmission Rate (%)													
(YR-MO-DAY)	*Channels:*	1	2	3	4	5	6	7	8	9	10	11	12	13	14
140112	Killeen Airport Food Court	0.00%	0.00%	0.00%	0.00%	0.00%	9.61%	0.95%	0.00%	0.00%	0.00%	0.19%			
140112	DFW Gate A36	0.55%	0.00%	0.00%	0.00%	0.00%	2.59%	0.00%	1.30%	0.00%	0.00%	7.88%			
140112	DFW Gate D20	0.96%	0.00%		0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	
140112	DFW Gate E21	2.22%	0.00%	0.00%	0.00%	0.00%	2.83%	0.00%	0.00%	0.00%	0.00%	3.10%			
140115	DCA Gate 30 & Food Court	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.36%	4.94%	0.00%	0.00%	
140115	DCA Gate 27 & Food Court	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	14.41%			
140115	DCA Gate 25	3.14%	0.00%	0.00%	0.00%	0.00%	0.19%	0.00%	0.00%	0.00%	0.00%	5.20%			
140115	DCA Gate 28	0.96%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	3.55%			
140115	DFW Gate B18	0.00%	0.00%	0.00%	0.00%	0.00%	0.52%	0.00%	0.00%	0.00%	0.00%	2.17%			
140119	Austin near Terminal Door	0.23%	0.00%	0.00%	0.00%	0.00%	2.63%	0.00%	0.00%	0.00%	0.09%	1.95%			
140119	Austin Gate 12	6.78%	1.40%	3.97%	0.00%	0.00%	0.77%	0.00%	0.00%	6.38%	1.01%	4.99%			
140119	DCA Gate 2		0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	3.88%			
140119	DCA Gate 9 - 1st Sample	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	1.14%	4.18%	0.00%	0.00%	
140119	DCA Gate 9 - 2nd Sample	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	12.42%			

Key

Blank – No transmission detected

0.00% – Data transmitted without errors

< 5% – Less that 5% retransmission rate

> 5% – More than 5% retransmission rate

ACRP

AIRPORT COOPERATIVE RESEARCH PROGRAM

Channel Utilization (% Occupancy)

Date	Location	2.4 GHz Band - Channel Utilization (%)													
(YR-MO-DAY)		1	2	3	4	5	6	7	8	9	10	11	12	13	14
130322	Atlanta Gate B22	8.1	10.2	1.6	12.9	13.3	12.4	10.2	7.2	5.0	4.5	3.4	2.5	1.5	0.2
130816	Chicago O'Hare Gate H5	7.1	7.3	5.9	4.7	5.0	5.1	5.1	5.2	7.2	9.0	9.0	8.0	5.1	0.1
130313	Nashville Gate A1	8.1	8.9	9.1	8.3	8.0	7.8	7.5	11.3	17.4	22.8	23.9	20.7	13.4	0.8
130814	DFW Gate A15	6.5	7.1	6.3	5.9	4.0	3.9	3.8	5.4	8.1	10.4	10.5	9.0	5.3	0.1
130509	Newark Gate A16	36.0	41.9	40.5	37.9	33.8	28.8	23.7	25.5	29.8	35.9	37.7	33.3	21.2	1.7
130403	Orange County Gate 14	11.9	11.4	8.1	4.1	4.1	4.3	4.1	3.2	1.6	1.1	0.9	0.7	0.4	0.1
130906	Austin Gate 8	6.8	7.3	7.3	8.8	10.1	10.4	10.4	16.6	24.0	32.5	35.6	30.6	21.1	0.8
131112	Austin Gate 9	14.3	14.3	12.0	6.9	6.2	6.1	4.6	3.1	5.4	7.0	6.8	6.5	3.6	0.6
131112	Midway Gate B2	15.3	16.0	13.2	10.5	9.7	9.7	10.5	11.8	13.4	16.3	16.6	13.1	8.8	0.7
131029	DEN Gate C33	21.0	23.5	21.6	21.3	19.3	15.9	14.0	12.9	12.8	15.6	16.4	14.8	9.8	0.6
131029	DEN Gate A37	7.0	6.7	5.8	7.9	9.3	9.7	9.7	7.3	4.8	4.5	4.4	4.2	2.6	0.5
131023	MSP Gate F1	66.1	63.9	58.5	49.9	37.2	28.5	17.0	10.3	8.8	9.7	10.1	8.9	6.1	0.8
131023	MSP Gate D4	11.0	11.6	11.6	11.4	11.2	11.1	10.7	8.9	8.6	9.9	9.8	9.0	5.5	0.4
131023	DEN Gate C40	10.7	11.3	10.3	10.1	13.0	14.4	13.9	13.0	16.4	20.4	20.7	19.8	12.8	0.4
131023	Copenhagen Gate C4	2.7	2.8	1.8	2.8	4.0	4.4	4.4	4.2	3.5	3.0	2.9	2.4	1.3	0.1
131023	Copenhagen Gate A2	5.7	5.2	6.3	7.1	7.3	8.1	7.3	4.8	2.9	1.4	1.1	0.8	0.5	0.0
140112	Killeen Airport Food Court	7.7	7.2	9.4	14.4	20.9	24.9	22.9	16.0	8.1	1.2	1.0	1.0	0.9	0.6
140112	DFW Gate A36	1.9	1.9	1.6	1.4	1.4	1.4	1.4	1.3	1.3	1.4	1.3	1.2	1.1	0.7
140112	DFW Gate D20	7.6	7.2	5.3	4.3	4.1	4.6	4.6	4.1	3.2	1.9	1.7	1.7	1.3	0.6
140112	DFW Gate E21	0.3	0.4	0.9	2.3	3.6	3.8	3.6	3.3	2.8	3.7	4.1	4.1	3.4	1.5
140113	NSF Keck Center Room 110	15.0	15.1	10.5	6.2	4.4	4.6	5.0	6.9	11.3	14.8	15.0	14.2	9.8	3.0
140115	DCA Gate 30 & Food Court	11.5	14.5	14.0	15.7	15.1	12.5	11.0	13.9	21.9	32.6	35.1	32.2	21.7	0.8
140115	DCA Gate 27 & Food Court	4.4	5.8	6.1	8.3	8.1	6.6	6.0	10.4	16.7	21.5	23.7	20.6	11.9	0.1
140115	DCA Gate 25	1.7	2.0	2.3	2.8	3.5	3.6	3.8	8.1	15.6	24.4	26.1	23.4	15.9	0.4
140115	DCA Gate 28	4.0	4.6	6.0	11.1	15.2	15.4	15.2	14.5	17.9	24.7	26.0	25.1	17.0	1.4
140115	DFW Gate B18	17.6	15.3	11.0	6.6	2.6	2.9	2.6	1.8	1.1	0.6	0.5	0.4	0.2	0.1

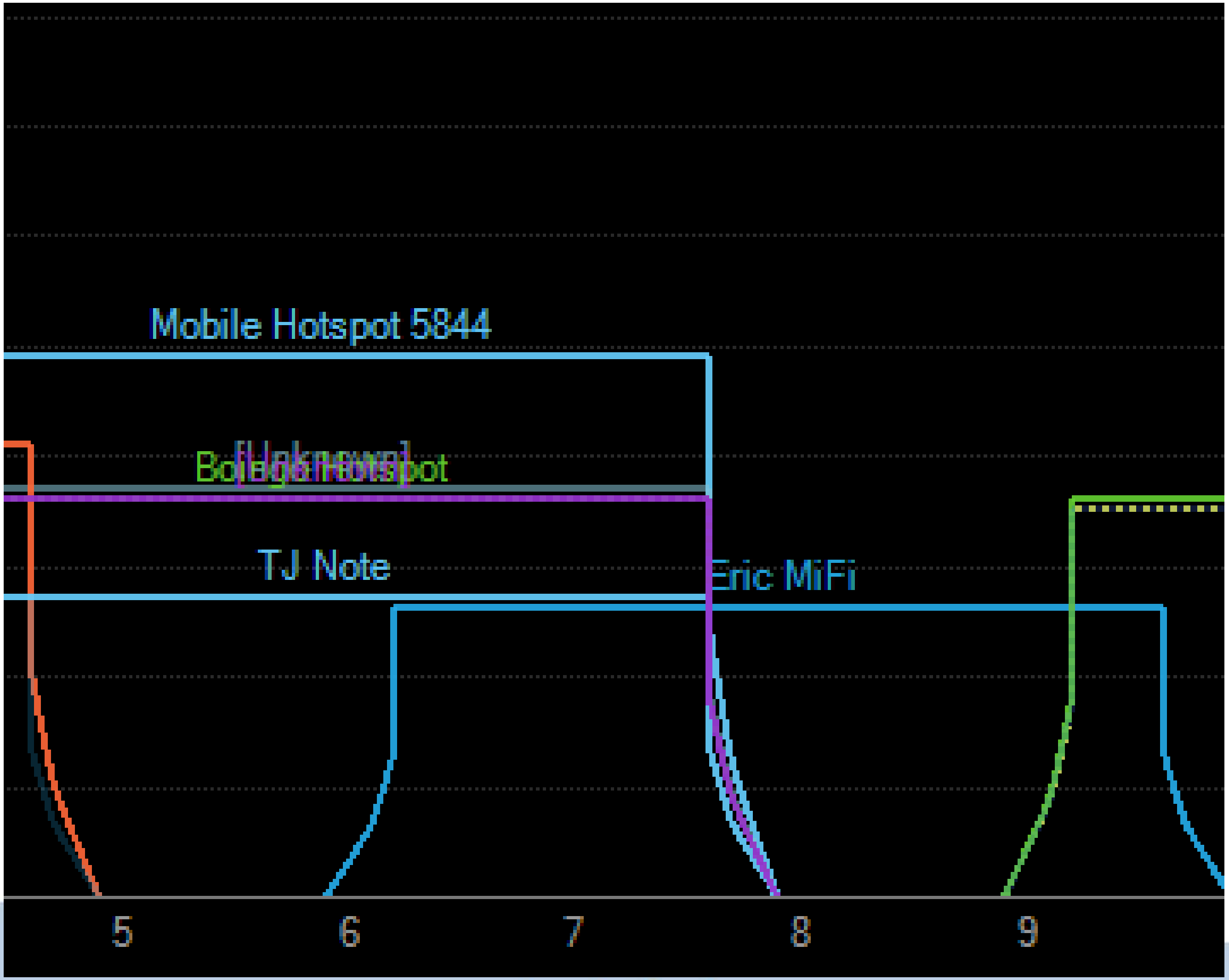
Key

0.00%	– Less than 2% utilization
2-20%	– 2% to 20% utilization
> 20%	– More than 20% utilization

ACRP

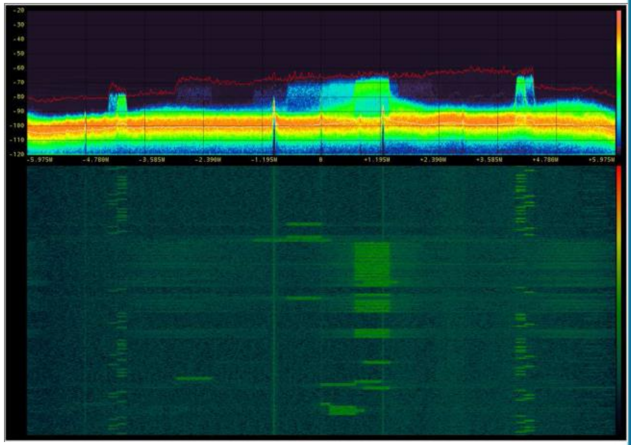
AIRPORT COOPERATIVE RESEARCH PROGRAM

Impact of Hotspots & Ad Hoc Networks



Automated Tools & Management

- Wi-Fi networks are too dynamic to manage manually
  - They require automated sensing and
  - New tools to manage them



- Software defined radio is providing a rich set of management tool
- Increasingly vendors are integrating these into their network products

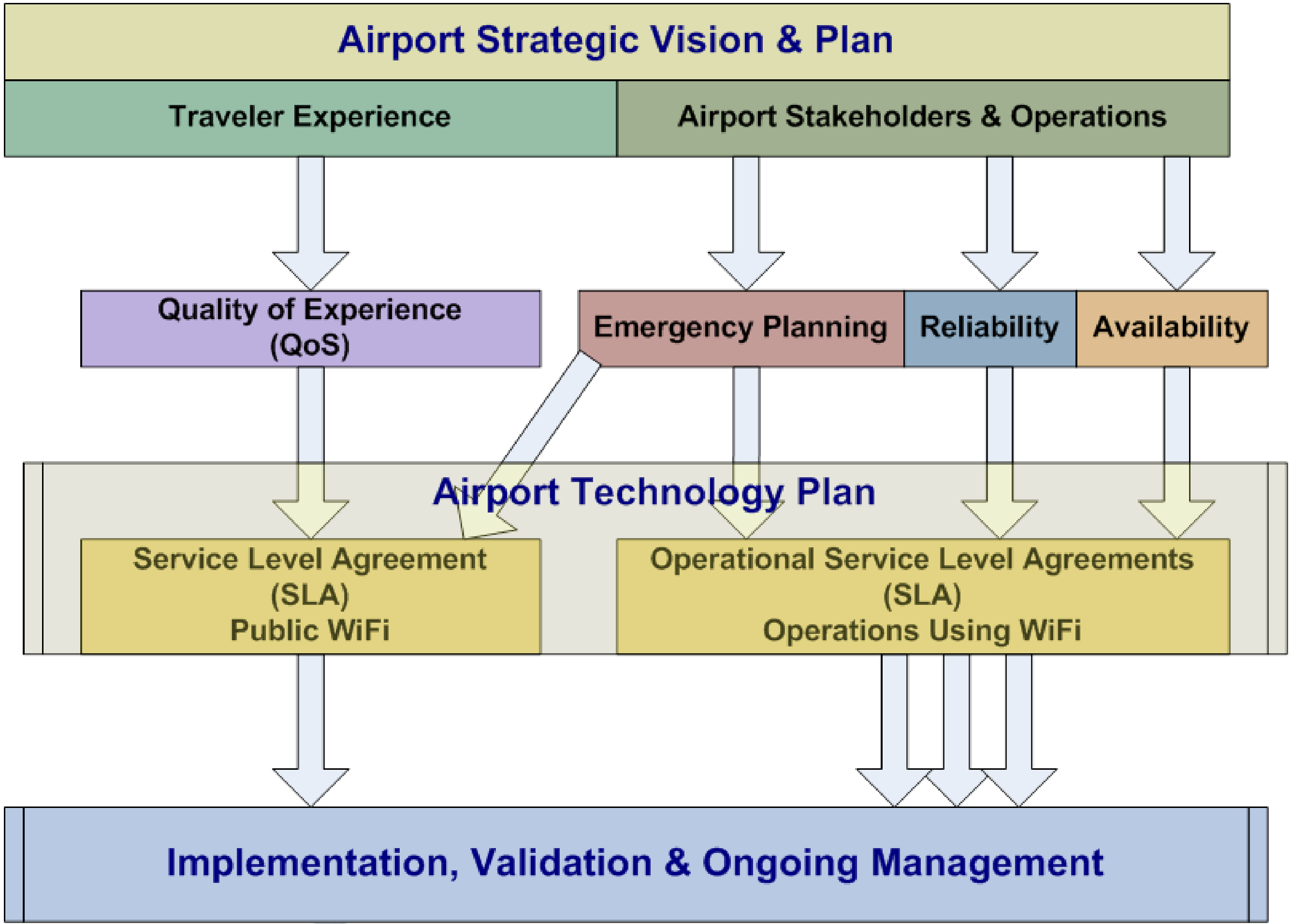
Strategic Planning for WiFi Networks

- Begins with an assessment and development of a robust network infrastructure
  - Existing systems
  - Future plans
  - Interdepartmental communication
  - Focus groups
  - Technology governance
- Develop an airport Strategic Plan
  - Similarities to public healthcare

    "The biggest mistake a healthcare delivery organization can make with wireless is failing to create a strategic plan on how to use and implement wireless technologies….Failure to create a foundational strategy increases the probability that the risks become adverse events."

AAMI Wireless Strategy Task Force, "FAQ for the Wireless Challenge in Healthcare," May 2014, question 4.

Sample Strategic Vision and Plan


Airport Strategic Vision & Plan
Traveler Experience
Airport Stakeholders & Operations
Quality of Experience (QoS)
Emergency Planning
Reliability
Availability
Airport Technology Plan
Service Level Agreement (SLA) Public WiFi
Operational Service Level Agreements (SLA) Operations Using WiFi
Implementation, Validation & Ongoing Management

ACRP

AIRPORT
COOPERATIVE
RESEARCH
PROGRAM

Service Providers Business Model

- Cellar business model:
  - Purchased dedicated “licensed” frequencies
  - Funded cost of establishing and operating networks
  - Subscribers provide funding to support the network
  - Decide and approve which devices are used on their networks; equipment certification process
- WiFi business model:
  - Operate in “unlicensed” spectrum
  - Networks are built in an ad-hoc manner; no single entity responsible for the network
  - Users determine which devices to bring to the airport; no regulated certification process before a device is marketed
  - Traveler expectation of free WiFi service at airports
  - Difficult to quantify user revenue source to support networks

Stakeholder Relationships and Business Model Options

- Airport stakeholders must work together regarding wireless services
  - Passengers, businesses, and airport operations
  - Television and other media
  - Security (physical and network)
  - First responders
- Master service level agreements (SLA): a means to tie all these relationships together
  - SLA enforcement
  - Shared tenet services
  - Alternative revenue sources
- Business model

WiFi Network Operations – Solutions

- Airport managers need processes and tools in place to monitor the network and ensure satisfactory operation
  - SLAs are one way to address this issue for airport managers, network operators, and all stakeholders
  - Network analytics – processes are only as good as the feedback and control systems that enforce them.
  - System performance oversight – involves ascertaining whether the right level and amount of resources are in place and then evaluating whether those resources are being used effectively
  - Network management structure – one dominant WiFi provider and possibly a second cellular provider, or it may consist of multiple WiFi providers each with their own competing network
- Emerging trend – internet of things (IoT) or internet of everything
  - Growing trend for many devices to be continuously connected to the internet – primarily to extract and analyze data in real time
  - Requires proactive management and strategic planning – as IoT continues to increase it will bring make it easier for airports to better handle traffic flows and customer needs seamlessly, but also create the potential for new problems, interference issues, and unintended consequences that need to be managed

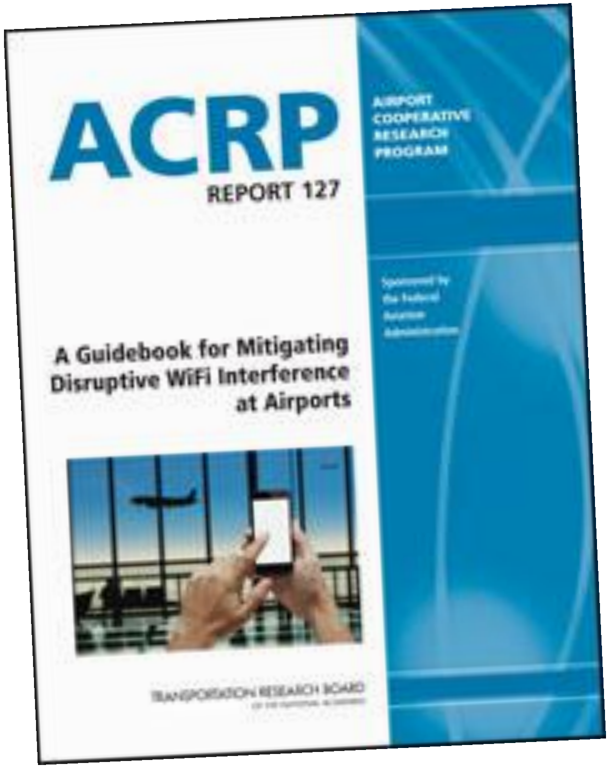
WiFi Operations at Small and General Aviation Airports

- Tend to be smaller, with typically simpler architectures, less traffic, and less dense requirements for WiFi services
  - Strategic plan is just as important even for scaled down wireless services with less available resources
  - Commercial publications are available that address the needs of small airports and can be tailored to meet requirements
  - One option is to build a system around a single carrier digital grid that enables high-speed broadband traffic that includes the airport proper and local community or town
  - SLAs can be used to define the stakeholder relationships, performance expectations, and cost sharing
- Process is similar to large airports
  - Identify the requirements
  - Quantify the desired service levels
  - Begin the design, time table for implementation, rough order magnitude for cost
- Establish and maintain data
  - Establish a database of problem reports and solutions
  - Take periodic measurements to assure performance

Conclusion – What Should Airport Managers Do?

- Remember primary airport WiFi interference is from other WiFi devices and passenger/stakeholder use cannot be restricted
- Will your business case take you into the future, does it mesh with your strategic plan, do stakeholders agree, and is it documented in some type of agreement?
- Consider making your network manager a strategic partner (not just a vendor); networks need to be periodically monitored, audited, and results compared to other networks and airports; and service providers require specialized skills to baseline and diagnose problems
- Does your crisis action plan include the WiFi network and appropriate security – loads change dramatically in any crisis situation

For additional information:



ACRP

REPORT 127

AIRPORT COOPERATIVE RESEARCH PROGRAM

Sponsored by the Federal Aviation Administration

A Guidebook for Mitigating Disruptive WiFi Interference at Airports

TRANSPORTATION RESEARCH BOARD
OF THE NATIONAL ACADEMIES

ACRP Report 127*:*
A Guidebook for Mitigating Disruptive WiFi Interference at Airports

http://www.trb.org/main/blurbs/172272.aspx

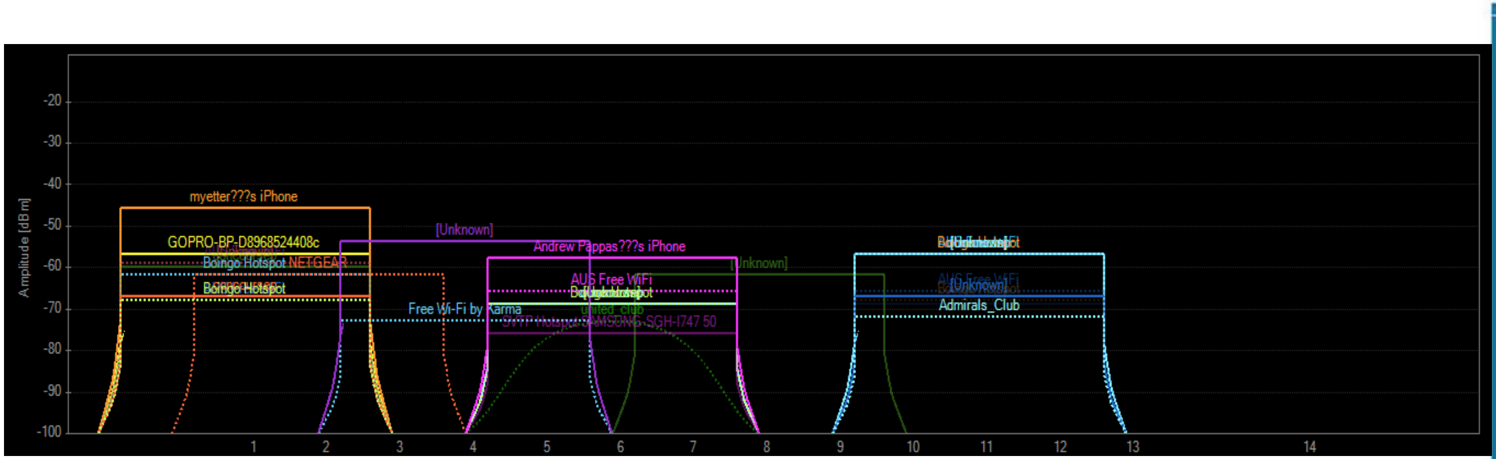
- Michael Carroll
  - mcarroll@sysplan.com
- Stephen Berger
  - stephen.berger@temconsulting.com

ACRP

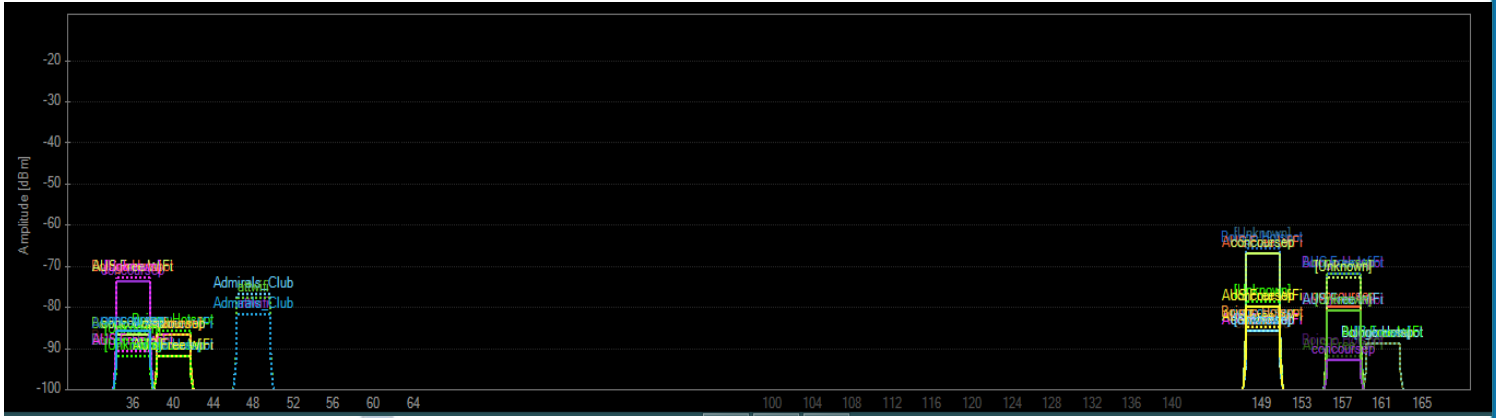
AIRPORT
COOPERATIVE
RESEARCH
PROGRAM

Supplemental Slides

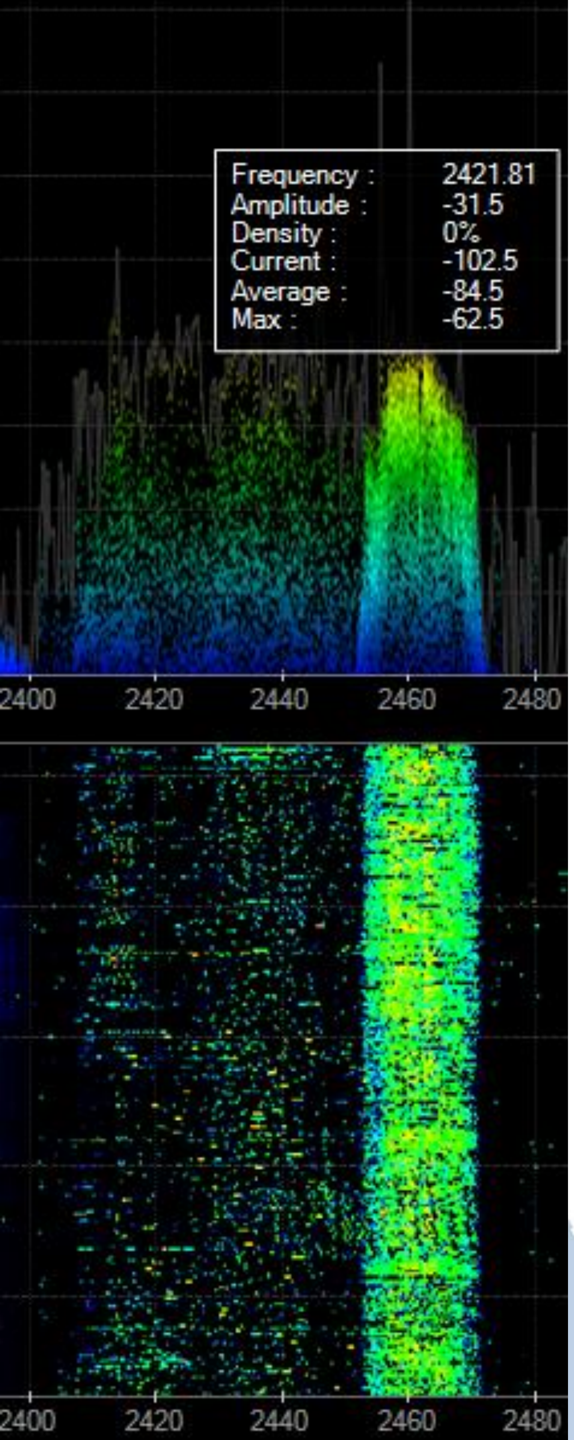
Spectrum Congestion
Use of 2.4 vs. 5 GHz WiFi Channels



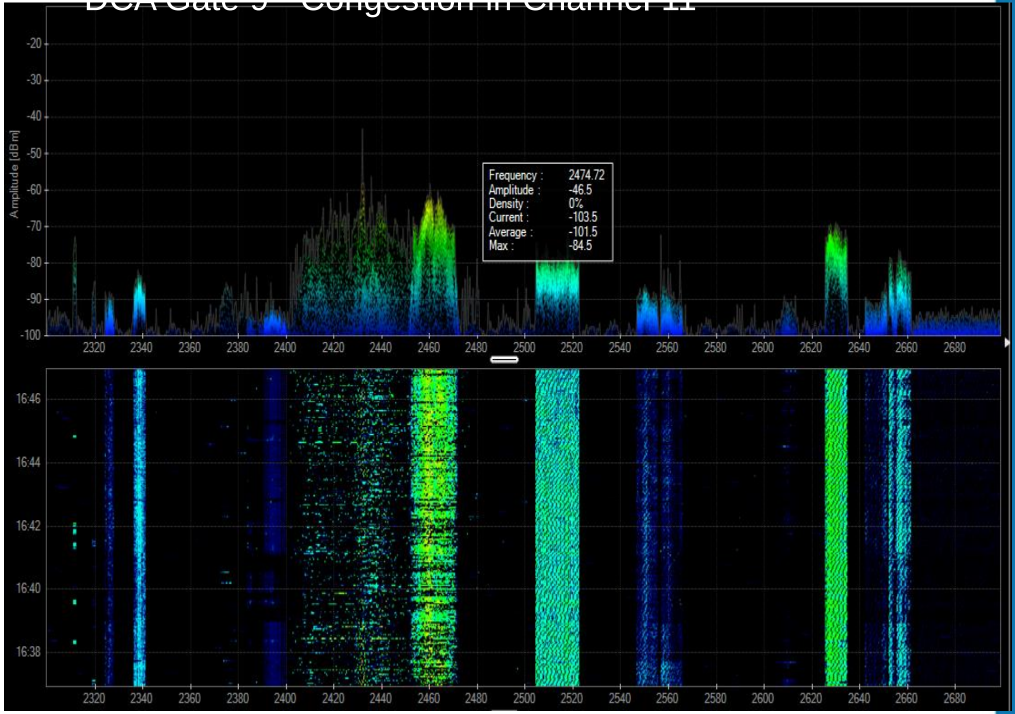
2.4 GHz



5 GHz


Frequency : 2421.81
Amplitude : -31.5
Density : 0%
Current : -102.5
Average : -84.5
Max : -62.5

DCA Gate 9 – Congestion in Channel 11


Frequency : 2474.72
Amplitude : -46.5
Density : 0%
Current : -103.5
Average : -101.5
Max : -84.5

ACRP

AIRPORT
COOPERATIVE
RESEARCH
PROGRAM

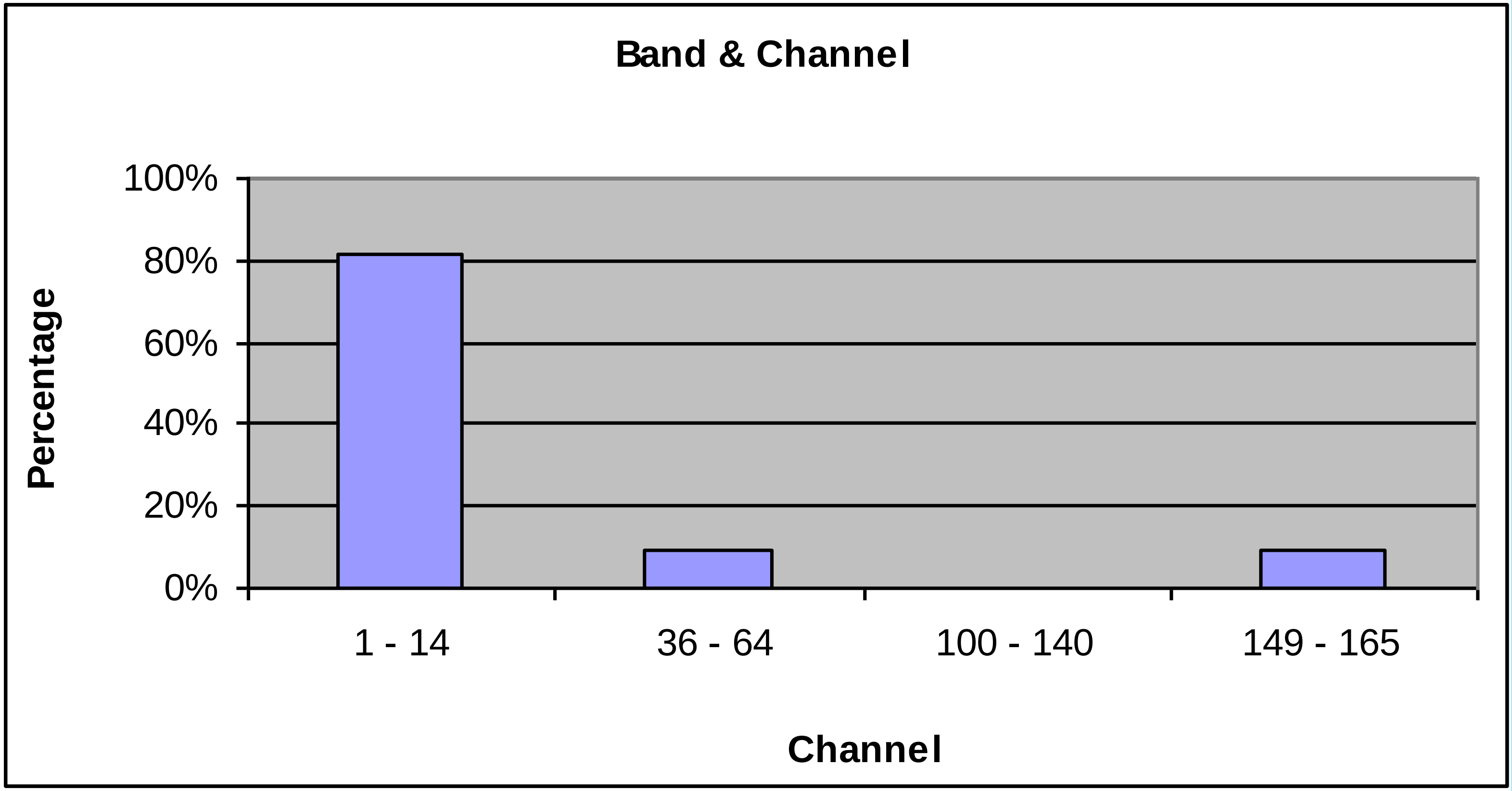
Traffic Distribution

Date	Location	Most Used Channel		Distribution by Band				
			Band:	2.4 GHz ISM	5.8 GHz Lower UNII, Indoor	5.8 GHz Lower UNII, DFS/TPC	5.8 GHz Middle UNII, DFS/TPC	5.8 GHz ISM
(YR-MO-DAY)			WiFi Channels:	1-14	36-48	49-64	100-140	149-165
131122	Philadelphia Gate D1	45.43%		99.98%	0.02%	0.00%	0.00%	0.00%
131122	Philadelphia Gate A9	26.00%		93.30%	3.58%	0.00%	0.00%	3.12%
131122	O'Hare Gate K4	28.75%		70.15%	11.50%	0.00%	0.00%	18.36%
131122	O'Hare Gate H5	33.93%		69.73%	18.44%	0.00%	0.00%	11.83%
131122	O'Hare Gate H5	44.07%		73.64%	15.88%	0.00%	0.00%	10.48%
131122	O'Hare Gate H9	30.54%		66.86%	12.76%	0.00%	0.00%	20.38%
131122	Austin Gate 12	22.41%		41.18%	40.21%	0.00%	0.00%	18.60%
131211	Waco Terminal B	31.33%		100.00%	0.00%	0.00%	0.00%	0.00%
140107	Austin Gate 12	61.02%		75.66%	12.99%	0.00%	0.00%	11.35%
140107	Denver Concourse C Food Court	26.26%		92.05%	5.37%	0.00%	0.00%	2.58%
140107	Denver Gate C28	27.64%		91.76%	3.64%	0.00%	0.00%	4.61%
140112	Killeen Airport Food Court	42.39%		100.00%	0.00%	0.00%	0.00%	0.00%
140112	DFW Gate A36	73.16%		89.10%	0.01%	0.00%	0.00%	10.88%
140112	DFW Gate D20	67.14%		26.17%	73.83%	0.00%	0.00%	0.00%
140112	DFW Gate E21	51.53%		78.55%	0.22%	0.00%	0.00%	21.22%
140113	NSF Keck Center Room 110	82.23%		95.08%	4.92%	0.00%	0.00%	0.00%
140113	NSF Keck Center Room 110	87.19%		99.57%	0.33%	0.00%	0.00%	0.09%
140115	DCA Gate 30 & Food Court	38.84%		54.45%	12.03%	0.00%	0.00%	33.52%
140115	DCA Gate 27 & Food Court	57.30%		81.66%	0.08%	0.00%	0.00%	18.26%
140115	DCA Gate 25	89.95%		100.00%	0.00%	0.00%	0.00%	0.00%
140115	DCA Gate 28	74.77%		83.03%	16.97%	0.00%	0.00%	0.00%
140115	DFW Gate B18	65.20%		90.22%	0.09%	0.00%	0.00%	9.69%
140119	Austin near Terminal Door C3D	43.13%		73.79%	14.01%	0.00%	0.00%	12.21%
140119	Austin Gate 12	33.53%		46.16%	35.86%	0.00%	0.00%	17.98%
140119	DCA Gate 2	97.85%		100.00%	0.00%	0.00%	0.00%	0.00%
140119	DCA Gate 9	58.94%		68.61%	0.09%	0.00%	0.00%	31.31%
140119	DCA Gate 9	64.86%		70.75%	0.02%	0.00%	0.00%	29.23%

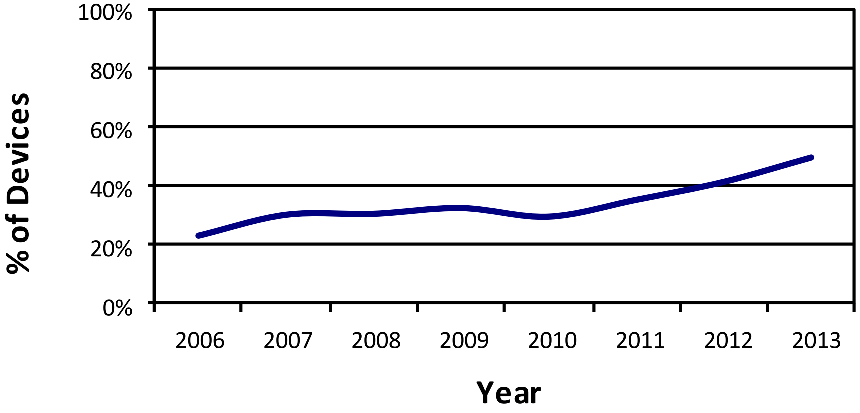
Key

0.00%	– No traffic
< 45%	– Less that 45% of total traffic
> 45%	– More than 45% of total traffic

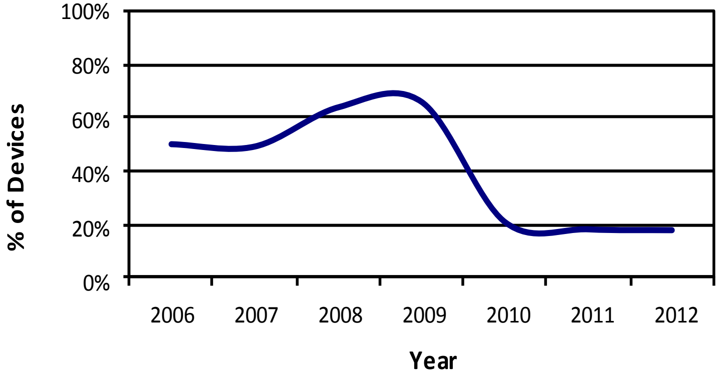
Band & Channel Distribution



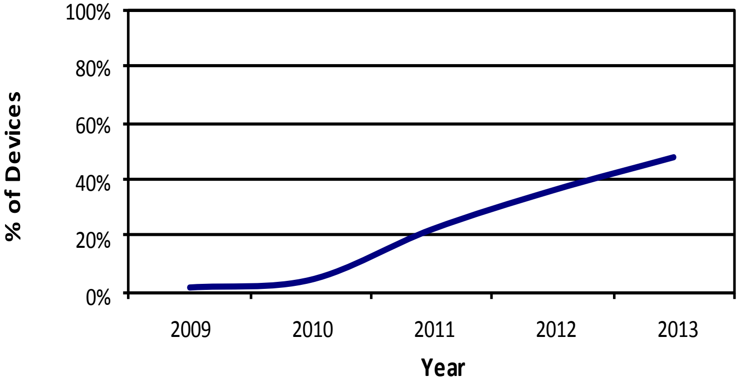
Dual Frequency Band Devices



Dual Frequency Band Laptops



Dual Frequency Band Smartphones



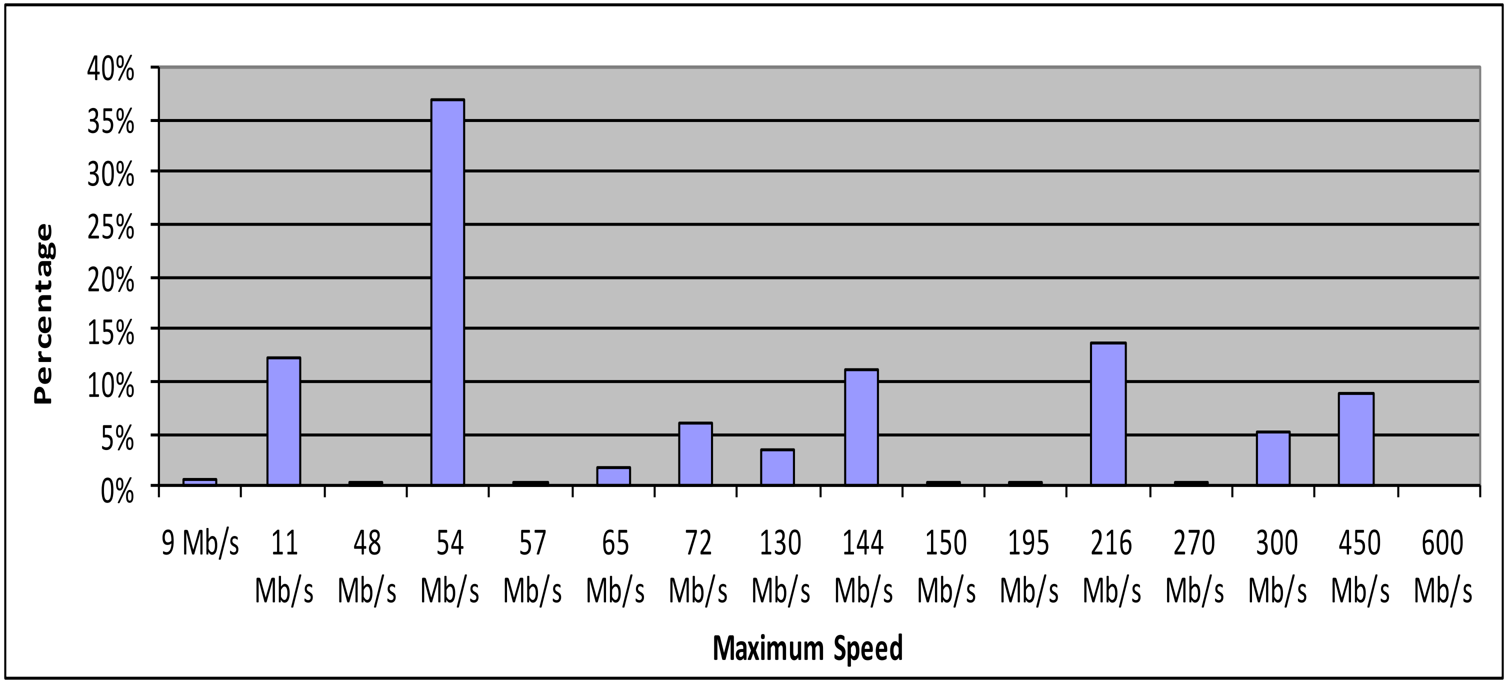
ACRP

AIRPORT
COOPERATIVE
RESEARCH
PROGRAM

Microsoft Featured Products, October 2013

Total number of **tablets**:	4
Number that are dual band:	2
Percent that are dual band:	50%
Total number of **laptops**:	15
Number that are dual band:	6
Percent that are dual band:	40%
Total number of **all-in-ones**:	7
Number that are dual band:	2
Percent that are dual band:	29%

Airport Access Points Data Rates



ACRP

AIRPORT
COOPERATIVE
RESEARCH
PROGRAM

Access Point Loading

Name	Access Points	Total Devices Detected	Devices/AP
Atlanta Gate B26	40	530	13.3
Atlanta Gate F1	38	311	8.2
Atlanta Gate F7	37	512	13.8
Atlanta Gate F14	27	500	18.5
Austin Gate 6	30	338	11.3
Amsterdam Gate D83	22	295	13.4
Amsterdam Gate C5	92	596	6.5
Amsterdam Gate D64	30	236	7.9
Amsterdam Gate E8	75	361	4.8
Amsterdam Gate D2	32	216	6.8
Amsterdam Gate D61	26	486	18.7
Copenhagen Gate A2	41	301	7.3
Copenhagen Gate C4	85	564	6.6
Copenhagen Gate D1	35	211	6.0
Minneapolis Gate D4	32	370	11.6
Minneapolis Gate F1	34	315	9.3
Denver Gate C40	24	353	14.7
Minimum	22	211	4.8
Maximum	92	596	18.7
Average	41.2	382.1	10.5
Standard Deviation	22.9	150.6	4.9

ACRP

AIRPORT
COOPERATIVE
RESEARCH
PROGRAM