

The Technology that Drives Government IT

AI & Automation Cybersecurity Cloud & Infrastructure Data & Analytics Smart Cities & IoT Emerging Tech State & Local

SHARE... E-MAIL THIS PAGE PRINTABLE FORMAT



Agency Award'Federal Aviation Administration | Protect and serve

BY WILLIAM JACKSON | OCT 07, 2007

Good security depends on people and as technology

Establishing a cybersecurity management operation requires more than just having the right tools in place. You also need the support of those above and below you in the chain of command. The Federal Aviation Administration's Cyber Security Incident Response Center grew from a small operation with limited capabilities into a departmentwide security management center because of the support the center received and the technology it uses.

'We've gotten buy-in from the senior leadership,' said Mike Brown, FAA director of information systems security.

The technology is important, too. Having a good security management tool to correlate the growing volume of information from network sensors is critical if an incident response center is to be useful to its customers, said Ron Maree, Northrop Grumman program manager for FAA's CSIRC.

'If it takes you 12 hours to get to something, you're too late,' Maree said. The task also requires cooperation with other organizations

SEARCH

STAY CONNECTED



[Advertisement]

A
2
P

SIGN UP FOR OUR NEWSLETTER.

Email Address

I agree to this site's Privacy Policy.

MOST POPULAR ARTICLES

DHS awards contract for AI-enabled CDM dashboard

Agencies warming up to AI

Is banning surveillance tech worth it?

The National Guard's cyber escape room

Defense against deepfakes

[Advertisement]

The Technology that Drives Government IT

AI & Automation Cybersecurity Cloud & Infrastructure Data & Analytics Smart Cities & IoT Emerging Tech State & Local

Some low-hanging fruit to show some return on investment.

'We work to gain constituent trust,' said Christopher Garcia, FAA program director for CSIRC. 'And once we get it we have to keep it.'

William Jackson

[Advertisement]



IN FRONT: Christopher Garcia says FAA's response center is



AIR DEFENSE: The CSIRC team network security covers the Transportation Department.

The Federal Aviation Administration's Cyber Security Incident Response Center recently changed its name, home and mission. As of Oct. 1, CSIRC became the Transportation Cyber Security Management Center, providing network security services for the entire Transportation Department from a new 15,000-square-foot facility in Leesburg, Va.

WHAT: Federal Aviation Administration Cyber Security Incident Response Center

MISSION: Provide the ability to protect FAA networks, detect intrusions and security incidents, respond to those incidents, and recover from them.

CHALLENGE: CSIRC began as a small team with few tools and responsibility for monitoring only the FAA administrative network. The evolution of air traffic control and other FAA operational networks away from stand-alone systems made them more vulnerable to network threats. The FAA CSIRC set out to provide more protection and to become a federal Center of Excellence for cybersecurity, providing services to other agencies.

SOLUTION: Beginning in 2001 with the arrival of Mike Brown as FAA director of information systems security, support from top-level management at FAA enabled CSIRC to build its resources and expand its capabilities with the addition of professional analysts, standardized intrusion-detection tools and a security information management system to provide analysis of data from the sensors.

IMPACT: Response time to security incidents has been reduced from hours to minutes, and CSIRC has become the Transportation Department's Cyber Security Management Center. It provides early warning and response to security problems for the department's networks and assists with vulnerability and

NEW FROM GCN

- Agencies warming up to AI
- The National Guard's cyber escape room
- DHS awards contract for AI-enabled CDM dashboard
- Defense against deepfakes
- Political parties vulnerable to cyber attacks

UPCOMING EVENTS

MAY 22

Face to Face: CDM DEFEND's New Approaches for Protecting Networks

The Willard InterContinental Washington, DC

MAY 31

A Market at the Crossroads: How M&A is Reshaping the World of Government Contractors

Valo Park McLean, VA

JUNE 26

FCW Workshop: Data Center Optimization - What Comes Next

The Willard InterContinental Washington, DC

JULY 17

Emerging Tech Summit

Willard InterContinental Hotel Washington, DC

AUGUST 7

Cybersecurity Summit:

Marriott Metro Center Washington, DC

The Technology that Drives Government IT

AI & Automation Cybersecurity Cloud & Infrastructure Data & Analytics Smart Cities & IoT Emerging Tech State & Local

[IMGCAP(1)]'Now we're getting out ahead of the curve' and managing security, said Christopher Garcia, CSMC program director.

The shift to departmentwide responsibility is one step toward the goal of establishing the FAA facility as a federal center of excellence for cybersecurity that could provide services to other civilian agencies on a fee-for-service basis. That would be the culmination of an effort that started six years ago to make a bare-bones incident response team in 2001 into a state-of-the-art security management center.

What began with three FAA employees and six contract support employees monitoring seven network sensors for the FAA administrative network is now an around-the-clock operation with 17 government watch employees supported by 33 contractors from Northrop Grumman. The center has its own testing and evaluation lab, a local-area network test bed and a training lab that uses a security information management tool to analyze data from a suite of network sensors. Center officials have signed memorandums of understanding to share information with Mexico, Canada, Europe and NATO, and would like to sign one with the United Kingdom, said FAA Information Systems Security Director Mike Brown.

'It's the largest thing that I've done in 27 years with the FAA,' Garcia said of the evolution.

[IMGCAP(2)]Garcia credits the arrival of Brown as security director from the Defense Department in 2001 as the catalyst for the transformation. Brown wanted to take the center from incident response to a full range of protection, detection, response and recovery. Northrop Grumman was brought in as an integrator in 2004 to help with the expansion.

1 2 next »

RELATED ARTICLES

Is banning surveillance tech worth it?
White House takes on cyber workforce gap
Symantec joins defense industrial base cyber program
Stop chasing ghosts and build a threat hunting strategy
How cybercrime feeds on modernization



MORE FROM 1105 PUBLIC SECTOR MEDIA GROUP

Campus Technology

Upcoming Events, Webinars & Calls for Papers (Week of May 27, 2019)

Survey: Competency-Based Model Excels for Nontraditional

Defense Systems

Coast Guard turns to DOD's new AI center for maintenance help

House renews call for multicloud JEDI

Federal Soup

View the May 27, 2019 FEND issue as a PDF

OPM reorg would outsource work to GSA

The Technology that Drives Government IT

AI & Automation Cybersecurity Cloud & Infrastructure Data & Analytics Smart Cities & IoT Emerging Tech State & Local

New ID policy looks to leverage government credentials

Report: States race to meet big data with Science Standards

Industry, government need to embrace the power of open standards

About Us Contact Us

DIGITAL EDITION ADVERTISE REPRINTS LIST RENTAL

©2019 1105 Media, Inc. View our Privacy Policy and Terms of Service