FACE TO FACE CYBER SECURITY

Sponsored by FOUR POINTS TECHNOLOGY A Service Disabled Veteran Owned Small Business RSA

Build a Strong CYBER ECOSYSTEM

Shutterstock

Effective cybersecurity demands attention from the top, but must begin with the basics.

EVENT OVERVIEW

Cybersecurity touches all aspects of an organization, not just information technology. Taking a holistic approach to cybersecurity and collaborating with others will help agencies build a strong cyber ecosystem. That approach can help agencies become more capable of withstanding attacks and other threats that affect their ability to deliver their mission.

The cybersecurity strategy of any agency should reflect this holistic approach and incorporate input from across the agency, according to government and industry experts speaking at a Feb. 17th event: Unified Security: Strengthening the Cyber Ecosystem.

For government agencies, this means focusing on basic cyber hygiene and workforce training. They also need to adhere to NIST security frameworks and get help from the Department of Homeland Security, invest in cyber tools, and create the appropriate cyber culture that incorporates security from the beginning, according to speakers.

There is a high probability that agencies will get hacked. While many breaches make the news, there are many others that don’t. Most hackers find a way into agency systems through relatively simple methods such as phishing attacks, missing patches or stolen passwords. As a result, basic cybersecurity practices truly matter, including proper employee training so everyone knows they're responsible for cybersecurity.

"The most sophisticated adversaries who attack us do not throw zero days at us every five minutes," says Richard Hale, Deputy CIO for Cybersecurity, DOD. They take advantage of misconfigured computers, an account without a password, or administrative privileges that weren't kept separate.

"If you don't have **cybersecurity on the frontal lobes** of most of your employees, it's going to be **a difficult haul."**

ROD TURK, CISO, COMMERCE DEPARTMENT

The DOD's primary cyber goal is mission dependability in the face of cyber warfare, says Hale. The department wants to raise awareness and accountability when it comes to cybersecurity. This includes accountability from the top down, redefined work roles, job descriptions, qualifications and training standards for the IT workforce.

DOD wants to do things differently with its network based on the incident data it collects, says Hale. This means not only using vulnerability data, but also looking at what the bad guys actually do to test whether or not there is appropriate protection in place.

Have You Been Hacked?

Most organizations don't even know they've been infiltrated until months after it happens. It takes more than 200 days on average before an entity realizes they have been hacked, says Rod Turk, Chief Information Security Officer, at the Commerce Department. What's more, 69 percent of them find out from a third party.

The goal is to reduce the "dwell time" says Turk, referring to the time an adversary has been operating within an organization's environment. The plan is to put tools, processes and procedures in place to reduce the dwell time and improve resilience. This doesn't work, he says, without the right people in place.

This might require a change in how people act, think and interact. "If you don't have the right culture in your organization, if you don't have cybersecurity on the frontal lobes of most of your employees, it's going to be a difficult haul," says Turk.

Putting the right governance structure in place is important as well. The business users must understand their role in ensuring cyber security and do so effectively. They have to use the security tools the way there were intended.

Governance isn't just management, although management is one component, says Steven Schmalz, Field CTO, Federal Division at RSA Security. "Governance is making sure all the various constituencies … know what they are supposed to be doing," he says. "They're working together, and are motivated to achieve the overall goal of the organization."

Security solutions and tools can help organizations as they work toward establishing a cohesive governance structure, says Schmalz . RSA and other vendors in the security space can provide agencies with tools that "make their lives easier" as they try and get governance up and running within their organizations.

The demands of the modern cybersecurity landscape require agencies to take a fully integrated approach, says Martin Stanley, Cybersecurity Assurance Branch Chief, Department of Homeland Security, Office of Cybersecurity and Communications. "In order to … make sure you are achieving the protection goals you have for a system or data or network or mission, (you must) take more of a full lifecycle approach."

DHS takes a fully integrated approach in providing cyber services to agencies and vendors, says Stanley. The department moves engineering cyber defense teams into the field to help agencies protect their systems, he says, and will propagate best practices and lessons learned.

The goal is to make people aware as early in the process as possible about the best way to talk about cybersecurity. Agencies should learn how to determine their needs, evaluate information gathered, put the controls in up front, understand how they work together and "stay true to that through the lifecycle of the system," says Stanley.

There are other resources agencies can turn to as well. One such resource comes from NIST, which drafted its Framework for Improving Critical Infrastructure Cybersecurity. This is designed to help organizations address cyber risks by aligning policy, business and technological approaches.

The framework is voluntary and evolving, just like cybersecurity, says Matthew Barrett, Program Manager, NIST Cybersecurity Framework. "We're trying our best to make (the framework) a valuable thing," he says. "We think it's a valuable thing and we are open to the fact that it might need improvements over time."

Service Disabled Veteran Owned Small Business
SDVOSB
cVE

FOUR POINTS
TECHNOLOGY

A Service Disabled Veteran Owned Small Business

RSA®

Intelligence-Driven Security Solution for Government

RSA provides Mission Critical Cybersecurity capabilities across the Federal Government.

First Source II

GSA

NASA SEWP
www.sewp.nasa.gov

Four Points Technology, LLC
14900 Conference Center Dr, Ste 100
Chantilly, VA 20151
703-657-6100 | rsasales@4points.com

NITAAC
OMB Authorized GWACs for IT Acquisition
CIO-CS
COMMODITIES/SOLUTIONS

www.4points.com

Session Highlights

Here are some take-aways from the individual sessions

SESSION 1

Cybersecurity: The Dwell-Time Factor

Speaker

Rod Turk, Chief Information Security Officer, Commerce Department

Rod Turk

“**The goal** at the end of the day is to **reduce the dwell time**.”

- Dwell time in cyber security means the time an adversary has been in your environment.
- It takes more than 200 days on average before an entity realizes they have been hacked; and 69 percent of those are notified by a third party.
- Dwell time touches training, policies, tools, and all aspects of IT. The goal is to reduce it.
- If agencies don’t have the right culture in place, cybersecurity will be difficult .
- Commerce is using the NIST framework and developing a cyber security culture so it’s in the forefront in everything it does, because cybersecurity touches all things IT.
- Agencies need to prepare for next exfiltration, much like the health care industry prepares for next health care crisis.
- It is cheaper and easier to bake the security into the program than to add it on later.
- Agencies need smart technical people, good writers and communicators to help reduce the dwell time.

SESSION 2

Partner Insights I

Speaker

Steven Schmalz, Field CTO, Federal Division, RSA

Steven Schmalz

“To get anything done, you have to make sure to **get the various constituencies** involved and in agreement as to **what they should be doing.**”

- Governance is not the same thing as management.
- Governance is making sure the various constituencies within an organization know what they are supposed to be doing, they’re working together and they’re motivated to achieve the overall goal of the organization.
- Organizations must have a governance structure in place so users understand their role in ensuring cyber security, do it effectively, and use security tools the way there were intended.
- Security solutions and tools can help organizations as they work toward putting a governance structure in place.

SESSION 3

Framework for Improving Critical Infrastructure Cybersecurity

Speaker

Matthew Barrett, Program Manager, NIST Cybersecurity Framework

Matthew Barrett

“**We’re trying our best** to make (the framework) a valuable thing. We think **it’s a valuable thing** and we are open to the fact that **it might need improvements** over time.”

- The Framework for Improving Critical Infrastructure Cybersecurity consists of three components: the core, the profile and the implementation tiers.
- The framework core includes vocabulary and a standardized library of cybersecurity outcomes, the profile is the customization of the core, and the implementation tiers component is a measurement of risk management practices.
- One of the ways to use tiers is a point of reflection: It shows how an organization implements the framework core functions and manages its risk.
- The core includes the five functions: identify, protect, detect, respond and recover.
- The profile lets people adopt and adapt the core as they see fit, based on given sector, subsector or organization.
- NIST is writing a publication designed to help agencies align the Risk Management Framework and the Cybersecurity Framework.

For more information on Face to Face Events go to: www.1105publicsector.com/events

Session Highlights

Here are some take-aways from the individual sessions

SESSION 4

Cybersecurity through Culture and Accountability

Speaker

Richard Hale, Deputy CIO for Cybersecurity, Department of Defense

Richard Hale

> "The most sophisticated adversaries who attack us **do not throw zero days** at us every five minutes. **They find misconfigured computers,** somebody **has an account** that doesn't have a password, or somebody **did not carefully separate administrative privilege.**"

- DOD's main cyber goal is mission dependability in the face of cyber warfare by a capable adversary.
- Other goals include: Safe sharing with other mission partners, common identity credentials, better insider threat protection, and protection of all embedded computing in DOD with appropriate cybersecurity.
- Misconfigured computers, missing patches, and overuse of passwords are some things that are easy to exploit but also easy to fix. Everybody is responsible for cybersecurity.
- DOD's cybersecurity discipline implementation plan revolves around accountability, and containing and slowing down the bad guys.
- Accountability from the top involving the boss in a meaningful way is important.
- DOD is redefining the work roles, job descriptions, qualifications and training standards for its IT workforce.
- DOD has to be clearer about cybersecurity requirements for weapons systems.
- DOD doesn't just want to use vulnerability data, but look at what the bad guys actually do to see if the cyber protection is appropriate.
- DOD is rolling out Windows 10.

SESSION 5

DHS Cybersecurity Capabilities

Martin Stanley, Cybersecurity Assurance Branch Chief, Department of Homeland Security, Office of Cybersecurity and Communications

Martin Stanley

> "In order to **provide cybersecurity** and to make sure you are **achieving the protection goals** you have for a system or data or network or mission, (you must) take **more of a full lifecycle approach.**"

- The DHS cyber vision is a fully integrated approach to provide services for federal and commercial organizations.
- CS&C focuses on helping secure the critical infrastructure of the .gov and .com domains, as well as maintaining interoperability and continuity of communications in the telecommunications space.
- It will move cyber experts with engineering expertise into the field to assist agencies in protecting their systems.
- DHS operates the Trusted Internet Connections, the Einstein system (national intrusion and detection system), and does penetration testing.
- The goal is to make people aware as early on in the process as possible about the best way to talk about cyber.
- Agencies should learn how to determine their needs, evaluate information gathered, put the controls in up front, understand how they work together and stay true to that through the lifecycle of the system.

> "The **DoD's primary cyber goal** is **mission dependability** in the face of cyberwarfare."
>
> **RICHARD HALE**
> **DEPUTY CIO FOR CYBERSECURITY, DOD**

For more information on Face to Face Events go to: www.1105publicsector.com/events

CYBERSECURITY AT THE PENTAGON

Cybersecurity's Human Factor: Lessons from the Pentagon

Shutterstock

The vast majority of companies are more exposed to cyberattacks than they have to be. To close the gaps in their security, CEOs can take a cue from the U.S. military. Once a vulnerable IT colossus, it is becoming an adroit operator of well-defended networks. Today the military can detect and remedy intrusions within hours, if not minutes. From September 2014 to June 2015 alone, it repelled more than 30 million known malicious attacks at the boundaries of its networks. Of the small number that did get through, less than 0.1 percent compromised systems in any way. Given the sophistication of the military's cyberadversaries, that record is a significant feat.

One key lesson of the military's experience is that while technical upgrades are important, minimizing human error is even more crucial. Mistakes by network administrators and users—failures to patch vulnerabilities in legacy systems, misconfigured settings, violations of standard procedures—open the door to the overwhelming majority of successful attacks.

The military's approach to addressing this dimension of security owes much to Admiral Hyman Rickover, the "Father of the Nuclear Navy." In its more than 60 years of existence, the nuclear-propulsion program that he helped launch hasn't suffered a single accident. Rickover focused intensely on the human factor, seeing to it that propulsion-plant operators aboard nuclear-powered vessels were rigorously trained to avoid mistakes and to detect and correct anomalies before they cascaded into serious malfunctions. The U.S. Department of Defense has been steadily adopting protocols similar to Rickover's in its fight to thwart attacks on its IT systems.

HEATHCARE CYBERSECURITY

5 Major Hospital Hacks: Horror Stories from the Cybersecurity Frontlines

In real-world war, combatants typically don't attack hospitals. In the cyber realm, hackers have no such scruples. "We're attacked about every 7 seconds, 24 hours a day," says John Halamka, CIO of the Boston hospital Beth Israel Deaconess. And the strikes come from everywhere: "It's hacktivists, organized crime, cyberterrorists, MIT students," he says.

Halamka was speaking on a panel about medical hacking at SXSW Interactive along with Kevin Fu, a University of Michigan engineering professor who studies medical device security. Together they told horror stories of major hospital hacks from recent years. Here are the top five different types of hospital intrusions:

1. Stolen medical records
2. Distributed denial of service attacks
3. Misdirected payments on fraudulent sites
4. Malware on Android devices
5. Ransomware attacks on hospitals

CIA VIEW ON CYBERSECURITY

The CIA Secret to Cybersecurity That No One Seems to Get

If you want to keep yourself up at night, spend some time reading about the latest developments in cybersecurity. Airplanes hacked, cars hacked, vulnerabilities in a breathtaking range of sensitive equipment from TSA locks to voting booths to medical devices.

The big picture is even scarier. Former NSA Director Mike McConnell suspects China has hacked "every major corporation" in the US. Edward Snowden's NSA leaks revealed the US government has its own national and international hacking to account for. And the Ponemon Institute says 110 million Americans saw their identities compromised in 2014. That's one in two American adults. The system is broken. It isn't keeping us, our companies, or our government safe. Worse yet, no one seems to know how to fix it.

How Did We Get Here?

One deceptive truth seems to drive much of the cybersecurity industry down a rabbit hole: If you keep bad actors and bad software out of your system, you have nothing to worry about.

Malicious actors target "endpoints"—any device or sensor connected to a network—to break into that network. Network security seeks to protect those endpoints with firewalls, certificates, passwords, and the like, creating a secure perimeter to keep the whole system safe.

This wasn't difficult in the early days of the Internet and online threats. But today, most private networks have far too many endpoints to properly secure. In an age of "Bring Your Own Device," the cloud, remote access, and the Internet of Things; there are too many vulnerabilities hackers can exploit.

VA CYBERSECURITY APPROACH

Does VA's Plan for Fixing Cyber Weaknesses Take Too Long?

The Department of Veterans Affairs' top tech official says the agency has a plan to close long-ignored watchdog recommendations for improving information security—but it'll take some time.

Testifying March 16 before the House Oversight and Government Reform Committee, VA Chief Information Officer LaVerne Council said her team plans to implement all recommendations identified by the agency's inspector general—some of them going back years—by the end of 2017. She aims to adopt about 30 percent of the recommendations by the year-end.

"We have made significant progress in improving our cybersecurity posture," Council testified, pointing in part to increased budgets. "For the first time, our security efforts are fully funded and resourced."

In its fiscal 2017 budget request, VA is seeking to nearly double its information security spending—from about $180 million to $370 million.

Council rolled out a new department-wide cybersecurity strategy last fall. In addition, during the 30-day "cybersecurity sprint" initiated by the White House after the massive Office of Personnel Management breach, VA exceeded targets for reducing the number of privileged users and implementing multifactor authentication.

NIST SURVEY

Survey: Majority of agencies follow NIST Cybersecurity Framework

With the rising tide of cybersecurity threats to government networks, one good sign is that the overwhelming majority of federal agencies are following guidance provided by the National Institute of Standards and Technology's cybersecurity framework.

> "We have made significant progress in improving our cybersecurity posture."
>
> **LaVerne Council, CIO, VA**

That's according to a recent survey, which found 82 percent of 150 IT and security professionals in the federal government said their agencies are either fully or partially implementing the NIST Framework for Improving Critical Infrastructure Cybersecurity. When broken down further, 53 percent are fully implementing, with 29 percent partially implementing the guidance. The survey was conducted by Dimensional Research and sponsored by Dell.

Created with input from more than 3,000 people from industry, academia and government, the NIST framework provides voluntary guidance for public- and private-sector critical infrastructure organizations to better manage and reduce cybersecurity risk. In addition to helping organizations manage and reduce risks, it was designed to foster uniformity in cybersecurity management communications.

NIST IMPROVEMENTS

NIST wants more feedback on cybersecurity framework

The National Institute of Standards and Technology is looking for more information on how its famed cybersecurity framework is being used by the private sector and what changes could be made to it in the future.

In a request for information posted Thursday to the Federal Register, NIST wants to learn how organizations are sharing the framework's best practices, what parts of the framework are utilized more than others and what sections need to be updated. "We're looking forward to receiving feedback on specific questions about its use and how it might be improved," said Adam Sedgewick, NIST's senior information technology policy adviser. The document was crafted after a year-long process and eventually released in 2014.

Earlier this year, cybersecurity experts told FedScoop the framework point has raised the cybersecurity conversation to the boardroom level at major corporations and critical infrastructure providers. Intel Corp. tested the framework at two of its major corporate divisions and found it provided enough benefit that it planned to expand use of it throughout 2015.