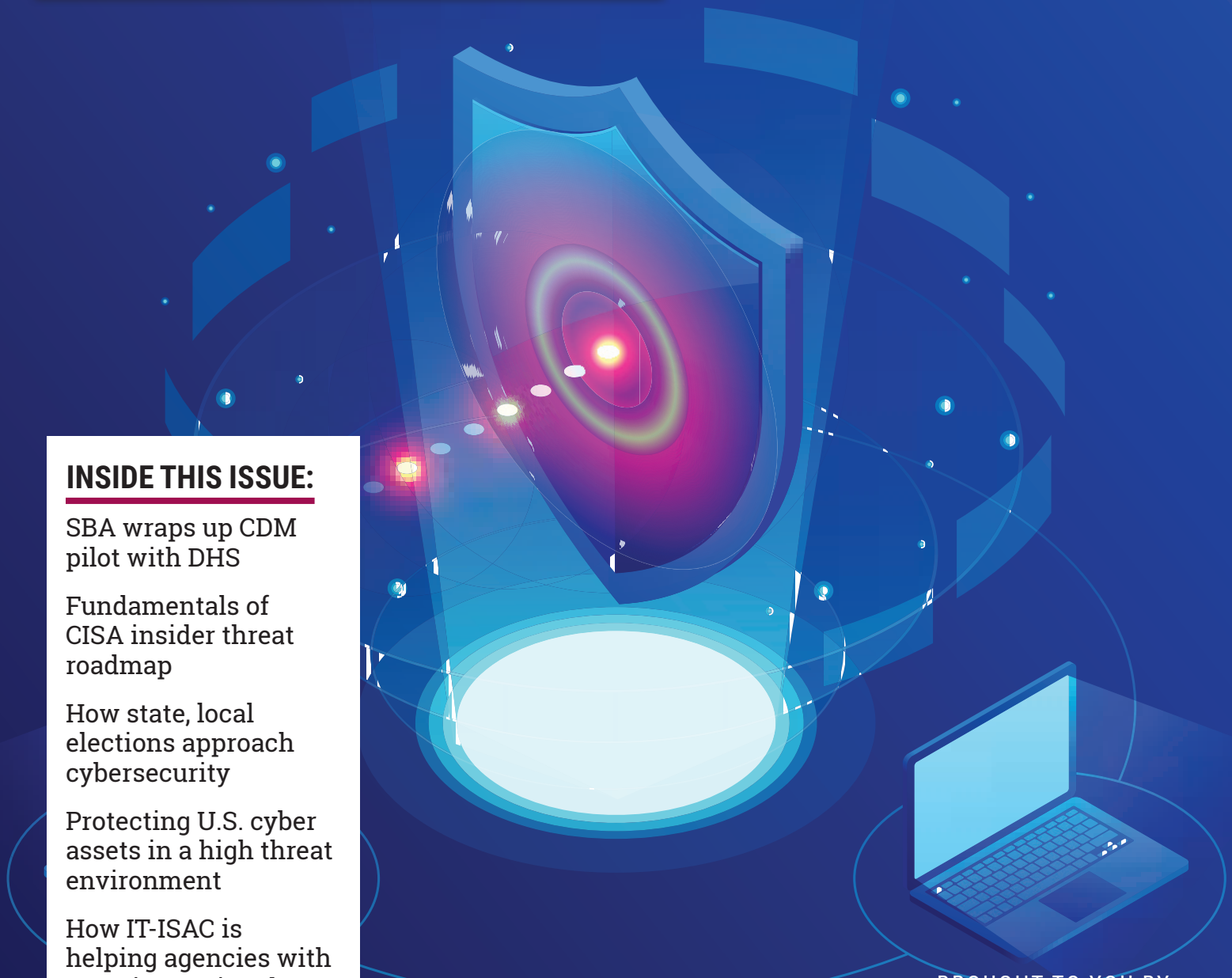
FEDERAL NEWS NETWORK

EXPERT EDITION

SECURITY STRATEGIES IN GOVERNMENT



INSIDE THIS ISSUE:

BROUGHT TO YOU BY:

ANOMALI®

ANOMALI®

Know Your Adversaries

Anomali® delivers intelligence-driven cybersecurity solutions. Organizations rely on the Anomali platform to harness threat data, information, and intelligence to make effective cybersecurity decisions that reduce risk and strengthen defenses.

Anomali arms security teams with machine learning optimized threat intelligence and identifies hidden threats targeting their environments. The Anomali platform enables organizations to collaborate and share threat information among trusted communities and is the most widely adopted platform for ISACs and leading enterprises worldwide.

Learn more: www.anomali.com

TABLE OF CONTENTS

With an ever-growing attack surface, it is impossible to know every single cyber threat or attack vector. But federal agencies have found the best defense is inside a culture of sharing.

The Department of Homeland Security leads the way with an evolving methodology to stay ahead of the crashing wave: continuous, careful exchange of information.

In this Expert Edition: Security Strategies in Government, we discuss a range of cyber efforts: from the EINSTEIN program's artificial intelligence that hastens threat sharing, to the Cybersecurity Vulnerability Identification and Notification Act that would compel internet service providers to turn over contact information for entities with critical cyber vulnerabilities.

Other highlights in this eBook:

- SBA's continuous diagnostics and mitigation (CDM) pilot with DHS to build out a cybersecurity dashboard provides an around-the-clock look at every device connected to the agency's network.
- How the IT Information Sharing and Analysis Center (IT-ISAC) and its membership of private-sector vendors work closely with DHS and other federal agencies on securing national critical functions.
- Agencies' opinion of and use of CISA's National Cybersecurity and Communications Integration Center (NCCIC), which has developed 43 types of products and services to help support the sharing of cyber threat intelligence.
- The Cyber Information Sharing and Collaboration Program that lets government and industry inform each other about current and future threats and attacks. And the new version of the Security Technical Implementation Guides (STIG), which facilitates sharing vulnerabilities at scale across the Defense Department.
- The "delicate balancing act on both sides" between government and the private sector to share critical information without giving away methods of obtaining that information.

The only way agencies and industry can try to stay ahead of the ever-evolving cyber threat is by acting as a team and realizing their survival against hackers is one of mutual trust and collaboration.

Lisa Wolfe
Editor-in-Chief
Federal News Network

SBA wraps up CDM pilot as part of enterprise IT transformation

BY JORY HECKMAN

Whether it's helping small businesses recover from natural disasters or just getting the word out about its services, the Small Business Administration deploys its personnel all across the country.

In order to give its employees in the field access to the data they need, Small Business Administration deploys the charge on cloud migration. Now the agency has wrapped up a continuous diagnostics and mitigation (CDM) pilot with the Department of Homeland Security to better secure its data.

Through the pilot, SBA has leveraged data analytics tools to build out a cybersecurity dashboard that provides an around-the-clock look at every agency device that's connected to its network, all the way down to mobile devices.

SBA's cloud-first approach to cybersecurity not only ensures that its desktops and servers get the latest software updates, but Maria Roat, SBA's chief information officer, said cloud-native tools have allowed the agency to stay "predictive" about activity on its network.

"If somebody goes on foreign travel and we don't know about it, we can see people logging in from other countries, getting ahead of what's going on in the environment," Roat said in an interview with Federal News Network. "Whether it's what threats might be against SBA – being able to see our entire inventory, who's on our network, what they're doing, how they're using our networks, and having visibility into that environment – that's something we did not have before."

SBA stands out as a leader in cloud migration, having advanced through all four phases of CDM.

But in terms of goals, Roat said her agency sees potential in using its cloud architecture to provide a "360-degree view" of its customers. That, combined with artificial intelligence or machine learning tools, could help the SBA anticipate the needs of more than 30 million small-business owners.

"If somebody gets a loan, and then they're looking at business plans, I can start using AI, if I have that customer model, to be predictive [and say] 'Oh, by the way, customer, here's what you might need next,'" she said.

In order to reach that 360-degree view of the customer, the agency has set into motion an enterprise IT transformation strategy that has laid as its foundation an overhaul of network identity access, employee productivity tools, data access and support services.

"Enterprise transformation, there's multiple pieces and parts to it, because it's not just about putting one tool in place. It's looking at the entire ecosystem of technology, as well as the people and processes to really drive that digital transformation we are in the midst of," Roat said.

This year, SBA has taken steps to implement an IT workforce strategy it completed in May 2018. Roat said the strategy includes teaching the workforce the basics of cloud, as well as data analytics and employee collaboration tools.

"Enterprise transformation [is] not just about putting one tool in place. It's looking at the entire ecosystem of technology ..."

MARIA ROAT, SMALL BUSINESS ADMINISTRATION'S CHIEF INFORMATION OFFICER

"As you spin up [virtual machines] in the environment, people need to understand how to operate in that environment," she said. "It's very different from being on-prem and having hardware that you're working on."

Through this IT transformation plan, Roat and her team have collaborated with SBA's chief data officer to develop an agency data lake for analytics and stood up a data community of practice.

"Certainly, my office and the relationship with the CDO is a partnership. We're working very closely together because I've got all these elements that I've put in place already, even before the advent of the law," Roat said.

The Foundations for Evidence-Based Policymaking Act, which President Donald Trump signed in January, mandated all agencies have until the end of July to appoint chief data officers and chief evaluation officers.

Other policy changes include an executive order the President signed in May 2018 giving agency CIOs direct hiring authority to fill critical skill gaps.

But before CIOs could take advantage of that new authority, the Office of Personnel Management had to send the proposed rule out for public comment.

"I am just now getting started on my vacancies to use that hiring authority," Roat said. "I've got a couple in the pipeline right now."

In the most recent Federal Information Technology Acquisition Reform Act (FITARA) scorecard, SBA stood out as one of just a few agencies that received an 'A' for their implementation of the Modernizing Government Technology Act.

Part of that, Roat said, comes down to her office and SBA's chief financial officer working closely with the Office of Management and Budget, as well as the agency's Office of Legislative Affairs to set up a working capital fund.

"Given where we are on the modernization trajectory, being able to do longer-term planning, instead of doing 12-month sprints … having the ability to look longer term over three years by turning that one-year money into three-year money, gives me a little bit more flexibility," she said.

Some agencies have faced an uphill battle with implementing the working capital funds, since they require a reprogramming of funds. While SBA remains in the middle of that reprogramming effort, Roat said the agency has identified several long-term projects to fund.

One major project is to consolidate all of the agency's IT service desks onto one platform. That's a major task because some service desks, Roat explained, only deal with problems with specific applications in certain program offices and have their own tracking management systems.

"I need to assess all of those service desks that are across the agency for those program-specific things and understand what they're doing, how they're responding, and then bring it onto an enterprise platform for an IT service, so that we're all using the same platform," Roat said. "That's going to take time because I've got to get the assessment done. I'm not one to eat the whole elephant at once, so I'm going to take small bites out of it and then start migrating those other service desks onto the platform."

SBA stood out as one of just a few agencies that received an 'A' for their implementation of the Modernizing Government Technology Act.

As CISA rolls out insider threat roadmap, industry experts highlight fundamentals

BY JORY HECKMAN

Agencies and private-sector companies invest considerable resources defending themselves against external cyber threats. But insider threats pose just as great a threat to these organizations if they don't have a strategy in place to defend against them.

In response to this threat, the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency released a private-sector toolkit in November 2019 to coincide with Infrastructure Month.

The document from CISA highlights insider threats as a top threat to critical infrastructure, and recognizes that these threats – both cyber and physical – can range from the theft of valuable data to sabotaging systems.

"There's no doubt in my mind that today we have individuals at work within our organizations [who] have the institutional knowledge as to how to bring us to our knees," Brian Harrell, the agency's assistant director for infrastructure security, said at CISA's Cyber Summit.

Security experts have said major organizations should already have an insider threat plan in place.

Randy Trzeciak, the director of the Insider Threat Center at Carnegie Mellon University's Software Engineering Institute, said an agency or industry insider threat program should start with identifying an organization's critical assets – in other words, identifying what technologies, facilities and people need the most protection.

Drilling down into those details, organizations can assign different levels of risk to traditional full-time employees, part-time employees, subcontractors, trusted business partners, cloud service providers, supply chain providers and other entities with authorized access to critical assets.

"You have insiders [who] have been granted authorized access, and your goal should be to prevent, detect, and to respond as efficiently as possible to insider threats to those critical assets," Trzeciak said.

Mark Weatherford, a global information security strategist for Booking Holdings, said identity management plays a key role in curbing insider threats, and allows organizations to detect when a user attempts to access facilities or networks that they wouldn't ordinarily access during the course of their workday.

"It's really about giving the right person the right access to the right things at the right time. We

have technologies today that allow us to do this with a very low lift," Weatherford said.

Cathy Lanier, the chief security officer for the National Football League and former chief of D.C.'s Metropolitan Police Department, said her current role requires her to take a converged approach to insider threats by bringing together physical security and cybersecurity personnel.

"The cybersecurity folks all want to use tools. The physical security folks all just want to go after and hunt down the bad guy. And what we want them all to do collectively is proactively prevent the bad guy from getting to us to begin with," Lanier said.

Frank Cilluffo, the director of Auburn University's McCrary Institute for Cyber and Critical Infrastructure Security, said the risk agencies and industry face from insider threats can't be overestimated.

"The greatest breaches of the past decade have been insider threats, more so than externally driven threats … the trusted insider has caused more harm to our national security from a theft of information and an intelligence perspective than anyone on the outside has," Cilluffo said.

"It's really about giving the right person the right access to the right things at the right time."

MARK WEATHERFORD, GLOBAL INFORMATION SECURITY STRATEGIST FOR BOOKING HOLDINGS

"The greatest breaches of the past decade have been insider threats, more so than externally driven threats."

FRANK CILLUFFO, THE DIRECTOR OF AUBURN UNIVERSITY'S MCCRARY INSTITUTE FOR CYBER AND CRITICAL INFRASTRUCTURE SECURITY

Stan Partlow, the vice president and chief security officer at American Electric Power, said managing insider threats is a matter of preparing for when, not if, it happens.

"The idea of preventing this is the proverbial unicorn. We're not going to prevent it because we allow these folks to have access to all of these areas. It's the most difficult challenge that any organization can face, because they're trusted," Partlow said.

While cybersecurity plays a significant role in any insider threat program, Trzeciak said leadership from other parts of the organization also needs to play a role.

"Information technology has a seat at the table, but equally important are other parts to the organization … human resources, personnel security, your general counsel within your organization. Physical security should be involved as well as the other key stakeholders to really integrate this into your enterprisewide risk program," Trzeciak said.

State, local elections officials agree no 'one-size-fits-all' approach exists for cybersecurity

With only a few months until the 2020 election, state and local election security personnel are gearing up to defend against cyber threats. While these officials work directly with the Department of Homeland Security to protect this critical infrastructure, in many cases they face limited resources on a scale not seen in the federal government.

More than 40 states have a secretary of state who serves as the chief election official, but in Wisconsin, an administrator is appointed by a bipartisan commission to serve in that role.

Meagan Wolfe, the administrator of the Wisconsin Elections Commission, said Wisconsin is the most decentralized election administration system in the country.

Whereas most other states run elections at the county level, Wisconsin runs elections at the municipal level. Resources for these offices can run thin and only two-thirds of Wisconsin's election officials work part-time.

"A lot of them don't have any type of IT support at the local level, which is very different than some of the county-based systems. The clerk might be the sole employee of that jurisdiction," Wolfe said at the Cybersecurity Coalition's CyberNext D.C. conference.

Lindsey Forson, the cybersecurity program manager at the National Association of Secretaries of State, said all 50 states cooperate with DHS on cybersecurity services, but the way states work with federal partners can vary greatly.

> **"Substantial progress has been made in terms of information sharing inter-governmentally [and] establishing the election infrastructure."**
>
> **LINDSEY FORSON, CYBERSECURITY PROGRAM MANAGER AT THE NATIONAL ASSOCIATION OF SECRETARIES OF STATE**

"A lot of states are working with their National Guards, but some states have many more legal constraints than others. Some states' guards are much more developed in terms of cyber teams than others," Forson said.

Although all 50 states work with DHS in some way, Forson said there is hesitation in some states about having the federal government scan systems and run penetration tests.

David Stafford, the supervisor of elections in Escambia County, Florida, said election security vendors need to understand the wide spectrum of resources individual counties may have for cyber defense.

"If you're coming to pitch something to Miami-Dade County, it's going to be very different than coming into a small or medium-sized county … a one-size-fits-all approach simply doesn't work," Stafford said.

Now more than ever, there is a plethora of federal resources for state and local election security officials, but Wolfe said it's important to know that those resources will remain sustainable in the years to come.

"What we always try to remind our locals about is that there is no finish line when it comes to election security. The goals, the objectives, the tools and resources that we use are going to change every single day. And if we get into the business of starting to say that there's going to be an end game, or there's one single goal, I think we'd be in trouble. That landscape does change on a daily basis," Wolfe said. "We want to set ourselves up for long-term success. The challenges we face for cybersecurity are not going to go away anytime soon."

Forson said states have made a lot of progress in election security since 2016, especially in getting individual states and individual jurisdictions to take steps to secure their systems.

"Substantial progress has been made in terms of information sharing inter-governmentally [and] establishing the election infrastructure," she said.

The Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC), she said, has also been a valuable resource for states. But building trust between various levels of government remains a challenge.

"We still do a lot of work around connecting our members to federal partners and getting questions answered about what is the FBI doing with the intelligence they receive. How do we get that? How do we ensure that the information is getting back out in a timely fashion? We're still doing a lot of work around that to improve that," Forson said.

State and local cyber officials continue to face challenges finding trusted vendors and research partners, but Wolfe said the key to building trust between the public and private sectors is to develop responsible partnerships.

"Cybersecurity is one of those arenas where you have the opportunity to really exploit people's fears and emotional responses … and leverage that to make a profit. I think it's always our hope, especially in this new landscape for elections security, that we're able to rise above a lot of that — to be able to responsibly partner in a way that gets states the things that they need … so that we can protect our democracy," Wolfe said.

> **"Cybersecurity is one of those arenas where you have the opportunity to really exploit people's fears and emotional responses."**
>
> **MEAGAN WOLFE, ADMINISTRATOR OF THE WISCONSIN ELECTIONS COMMISSION**

How to protect U.S. cyber assets in a high threat environment

THIS CONTENT HAS BEEN PROVIDED BY ANOMALI

Tensions may be slightly calmer between the United States and Iran, but in the cyber world, the stakes are always high between the two countries.

That's why the United States must rely on threat intelligence to stay ahead of adversaries like Iran, who are constantly trying to find a way into critical assets.

"Where we see a bigger risk from Iran is on the cyber front. This shows how war has evolved. It used to be very focused on your kinetic and nuclear power. As we've become an interconnected world connected by the internet, cyber became a higher risk target and the barrier for entry is much lower," Jill Cagliostro, project manager at Anomali, said as part of the series Security Strategies in Government, sponsored by Anomali.

It isn't expensive to train a cadre of hackers in comparison to buying a fighter jet.

"You need a computer and an internet connection and from there you can cause a lot of destruction," Cagliostro said.

So how does the United States get the intelligence it needs on threats and stay ahead of actors like Iran?

According to Cagliostro, it all starts with threat training. Humans will always be the weakest link in a security stack since they will always need to enter a username and password, which makes those credentials easily compromised.

> "One of the best ways U.S. entities can prepare is to remind their users how to defend themselves against phishing attacks, to be more vigilant and to put all of their users on high alert that these things may be coming in."
>
> **JILL CAGLIOSTRO, PROJECT MANAGER AT ANOMALI**

"One of the best ways U.S. entities can prepare is to remind their users how to defend themselves against phishing attacks, to be more vigilant and to put all of their users on high alert that these things may be coming in," Cagliostro said.

Another way U.S. organizations can deter attacks from Iran or any hackers is to share information. The United States set up the Cyber Information Sharing and Collaboration Program so government and industry can inform each other of threats and attacks. There is also a new version of the Security Technical Implementation Guides, which facilitates sharing vulnerabilities at scale.

"The new model allows for a lot more flexibility and a lot more detail and the ability to capture relationships between pieces of information," Cagliostro said. "By formalizing the way we share information and ingest this information, it makes it much easier to track at scale and take action on. The future of threat intelligence is model first. It's focusing on identifying tactics techniques and protocols [and] the actor groups. It's looking at that higher level and making sure you're protected."

"The Department of Homeland Security has done a very good job of making it easier to share in smaller communities, so there is less risk of attribution, it's a small vetted audience and you feel more comfortable."

JILL CAGLIOSTRO, PROJECT MANAGER AT ANOMALI

Still, industry has had some issues when it comes to sharing information. No one wants to admit they have vulnerabilities, Cagliostro said.

"Sharing is inherently a scary thing for companies both on the commercial side and on the federal side," she said. "When you share out intelligence it's essentially admitting, 'I've seen this in my environment.' There's a very, very high fear of attribution back to them. The Department of Homeland Security has done a very good job of making it easier to share in smaller communities, so there is less risk of attribution, it's a small vetted audience and you feel more comfortable."

IT-ISAC seeing 'a lot more engagement' from federal government on cyber threat intelligence

BY JORY HECKMAN

> **"One of the challenges in cyber threat intelligence is that there really is no common understanding of what we mean by that term."**
>
> **SCOTT ALGEIER, EXECUTIVE DIRECTOR OF THE IT INFORMATION SHARING AND ANALYSIS CENTER**

The Department of Homeland Security and its partners have taken significant steps in recent years to formalize the process of sharing cyber threat intelligence (CTI) with private-sector companies to protect the nation's critical infrastructure.

Despite these signs of progress, the concept of cyber threat intelligence and what it means for agencies and industry remains difficult to define.

Scott Algeier, the executive director of the IT Information Sharing and Analysis Center (IT-ISAC), said in an interview with Federal News Network that cyber threat intelligence is a useful tool for agencies and industry leadership once they're on the same page about what it entails.

"One of the challenges in cyber threat intelligence is that there really is no common understanding of what we mean by that term," Algeier said in an interview with Federal News Network.

While the membership of ISACs consists of private-sector vendors, these ISACs work closely with DHS and other federal agencies on securing national critical functions. Through those partnerships, Algeier said he's noticed an effort within agencies to share more sensitive threat indicators more quickly.

Overall, we're seeing a lot more engagement from the government to industry, when there are specific threats that they want industry to be aware of," Algeier said. "We're seeing more analytical reports from the federal government that are actionable, that provide information that our members can use to manage threats against their networks."

The IT-ISAC and its partners, for example, have recently worked with agencies that deal in highly classified environments and have been provided malware samples and other sensitive information.

"We're seeing pretty good collaboration across the board between industry and government," Algeier said.

That collaboration, he added, will only improve with time. Within the IT-ISAC, for example, vendors have banded together to form special interest groups focused on security intelligence and sharing best practices on CTI.

> **"Coordinated vulnerability disclosure programs help improve the security of systems by helping vendors and government agencies identify and mitigate vulnerabilities."**
>
> **SCOTT ALGEIER, EXECUTIVE DIRECTOR OF THE IT INFORMATION SHARING AND ANALYSIS CENTER**

"We're bringing in the lead analysts from our member companies, who have the responsibility for finding the sophisticated [cyber] actors within their environments. They're sharing with each other about tactics they use, techniques they use, how they're finding incidents," Algeier said. "And this, of course, serves as a multiplier effect. Now other companies can learn from their experience [and] can learn from what they've done."

The threat intelligence community also has seen greater use of automation and machine learning tools to streamline information sharing – moving away from copying and pasting information from spreadsheets and moving toward rapid machine-to-machine sharing of information.

"I'm hopeful we can have members share with each other and how they are leveraging those tools, and talk with each other about how they're implementing AI and machine learning within their environments," Algeier said. "This knowledge sharing can increase the capabilities across our membership in the future."

Automation could also free up threat analysts to focus more on how best to mitigate threats once they've become known.

"A lot of the requests we're getting from members is how they can prioritize indicators that we're providing them. So we'll be spending some time in the short term to assist them with that," Algeier said.

Beyond the front-line threat analysts, executives both in government and industry have expressed a need for comprehensive, strategic, risk-based data to support their decision-making and mitigate operational threats.

"It's important to understand there's a larger audience for cyber threat intelligence – the senior-level executives who need to make strategic risk-management decisions," Algeier said.

In one notable case, civilian agencies will soon adopt a CTI best practice from the private sector: vulnerability disclosure policies.

Last November, the Cybersecurity and Infrastructure Security Agency and the Office of Management and Budget notified agencies that they'll soon be required to develop vulnerability disclosure policies, making it clear that agencies welcome good-faith security research on specific, internet-accessible systems.

Algeier said these coordinated vulnerability disclosure programs have been successful in the private sector, and appear to be a step in the right direction for agencies.

"One of the key values of a coordinated vulnerability disclosure program is that it helps mitigate the risk to end users. If a vulnerability is announced before a fix is available, the end user is placed at greater risk," Algeier said. "Coordinated vulnerability disclosure programs help improve the security of systems by helping vendors and government agencies identify and mitigate vulnerabilities."

GAO sees DHS stepping up to provide cyber threat intelligence to partners more quickly

BY JORY HECKMAN

The Department of Homeland Security's Cybersecurity and Infrastructure Security Agency looks to make 2020 the "year of vulnerability management" for its federal agency partners to further cement its role as the federal government's cyber coordinator.

But even with this in the works, Greg Wilshusen, the director of information security issues at the Government Accountability Office, said barriers still stand in the way of agencies sharing cyber threat information with each other and with their partners in the private sector.

At the same time, he said, DHS has come a long way in improving its cyber threat information sharing. When GAO surveyed owners and operators of national critical infrastructure only a few years ago, only about 28% of respondents said the federal government was providing actionable, timely and useful cyber threat intelligence.

"There's a challenge in making sure that we get that information, or that they provide that information to DHS," Wilshusen said.

In a more recent survey from February 2017, GAO has found respondents had expressed a more

favorable opinion of CISA's National Cybersecurity and Communications Integration Center (NCCIC), which has developed 43 types of products and services to help support the sharing of cyber threat intelligence.

"They're much more favorably inclined and appreciate the products and services that DHS was offering in this respect," Wilshusen said about those survey results. "So at least there's been some progress going forward on the part of DHS."

"There are often wide gaps in the implementations of their capability to view their entire network and the activity that's actually occurring on their network."

GREG WILSHUSEN, THE DIRECTOR OF INFORMATION SECURITY ISSUES AT THE GOVERNMENT ACCOUNTABILITY OFFICE

GAO's work has also identified some of the challenges that DHS has had in terms of providing cyber threat intelligence to the private sector as well as other federal agencies.

"In some cases, some of these entities didn't have the security clearances in which to receive some of the information that the government had that could be shared," Wilshusen said.

In other cases, GAO raised concerns the cyber threat intelligence that is shared is appropriately anonymized, so that sensitive information can't be connected to specific individuals or entities.

But GAO has also seen some positive trends, including further clarification of the roles and responsibilities the federal government and its partners have in collecting and sharing cyber threat intelligence.

Wilshusen said GAO has also seen improved communications and coordination between DHS and the intelligence community, which puts the federal government in a better position to share cyber threat intelligence with its partners.

Another recent trend Wilshusen noted is an effort to speed up the overall process of sharing cyber threat intelligence.

"One of the problems in the past is that often the information DHS might have provided out to entities through technical alerts was not necessarily very timely. Other private-sector organizations may have already addressed some of the vulnerabilities and the threats based upon information from some of the security contractors and providers [already] out there," he said.

As part of these positive trends, DHS has taken some early steps to automate the sharing of cyber threat information through systems like EINSTEIN to examine incoming network traffic and screen for cyber threats.

The success of these tools, Wilshusen said, has also led to a conversation about using artificial intelligence tools in the sharing of cyber threat intelligence.

"You have these advanced algorithms that can help cybersecurity professionals in a variety of ways," he said. "The key benefit is that it helps reduce the time and effort it takes to perform these different tasks – like identifying vulnerabilities and patching vulnerabilities [or] even detecting attacks and defending against active attacks," Wilshusen said. "The automation of that and being able to use machine learning to an extent can help cybersecurity professionals."

These AI and machine learning tools, he added, could serve as a force multiplier for cybersecurity professionals in terms of expanding their auditing and monitoring capabilities.

"There are often wide gaps in the implementations of their capability to view their entire network and the activity that's actually occurring on their network," Wilshusen said. "And the information they do collect, it's still often very voluminous. They just don't have the time or the expertise to actually look at that type of system activity and the audit logs or system logs. Usually, they're only looking at that when an incident has occurred."

Heightened vigilance amid Iranian cyber threat 'a new normal' for agencies

BY JORY HECKMAN

Increased tensions between the U.S. and Iran last December kept agencies on high alert over the threat of an Iranian cyber attack. Even as those tensions cooled, cybersecurity officials have warned agencies to remain vigilant.

David Springer, a former counterterrorism planner and intelligence officer at the Defense Intelligence Agency, now an associate at the law firm Bracewell, said agencies will remain in a heightened state of cyber awareness for months to come.

"Iran is a persistent threat and will continue to be a persistent threat in this space. There are obviously other high-end threats out there, and a lot of the same steps agencies can take against those other threats also are helpful in defending against malicious Iranian activity," Springer said. "I don't think this is, by any means, going away from the front of people's minds."

As far as the "very real and enduring threat" that Iran poses, Springer said agencies and the private sector should remain vigilant against mid-to-low level attacks that would deny access to systems for a limited period of time, steal valuable data or deface public-facing websites.

Iran also remains capable of standalone disinformation campaigns that can promote misleading information online, or "hybrid" attacks that combine disinformation with a cyber attack to create increased confusion.

"When you talk about hybrid use of cyber, there certainly is a concern that you can have a mixed cyber and physical real-world attack, where a threat actor can use cyber to either amplify the effect of some real-world terrorist or military action or create conditions that allow that real-world physical attack to take place," Springer said. "I think those are both issues agencies have been aware of for a while and will continue to be very vigilant about."

Making 2020 the 'year of vulnerability management'

The looming threat of a cyber attack from Iran prompted the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency to issue a memo warning that Iran and its proxies "have a history of leveraging cyber and physical tactics to pursue national interests, both regionally and here in the United States."

While that memo brought agencies to a heightened sense of vigilance, Springer said agencies will likely remain on guard for the foreseeable future.

"I think this is a new normal, or potentially just a reinforcement of the normal that's been the case for a few years. A malicious cyber activity, whether it's

> **"Iran is a persistent threat and will continue to be a persistent threat in this space."**
>
> **DAVID SPRINGER, FORMER INTELLIGENCE OFFICER AT THE DEFENSE INTELLIGENCE AGENCY AND CURRENT ASSOCIATE AT BRACEWELL**

> **"The federal government has really made strides in information-sharing with the private sector, [but] there's still more work to be done,"**
>
> **DAVID SPRINGER, FORMER INTELLIGENCE OFFICER AT THE DEFENSE INTELLIGENCE AGENCY AND CURRENT ASSOCIATE AT BRACEWELL**

from Iran or another sophisticated nation-state is just a perpetual problem," he said. "And I think heightened vigilance is certainly warranted when there's a particular geopolitical event that makes a more imminent action more likely."

Meanwhile, CISA set plans late last year to make 2020 the "year of vulnerability management," and further cement its role as the federal government's cyber coordinator. And early this year, the agency has already acted on that mission.

The agency, on Jan. 14, put out an emergency order to address known vulnerabilities in Microsoft's Windows operating system. The directive gave agencies mere days to assess the scope of the vulnerability to its systems, and 10 days to patch or remedy all its affected endpoints.

The patch released by Microsoft addresses vulnerabilities discovered by the National Security Agency that affect Windows' cryptographic functionality.

Springer said that coordinated response demonstrated growth in the federal government's ability to share cyber threat intelligence with the private sector in real time to mitigate vulnerabilities. More importantly, he said it showed that the federal government is "more willing to work with the private sector and reveal certain vulnerabilities rather than just keep them secret and use them."

"The federal government has really made strides in information-sharing with the private sector, [but] there's still more work to be done," he said. "It's not perfect, there are still concerns on both sides of exactly how much to share and when, but I think there's no question that it has been improving over time."

Meanwhile, Congress has taken steps to improve the legal framework for sharing cyber threat intelligence. The House Homeland Security Committee in January approved the Cybersecurity Vulnerability Identification and Notification Act, which would give CISA administrative subpoena power.

That authority would require internet service providers to turn over contact information for entities that CISA has identified as having critical cyber vulnerabilities.

However, Springer said there's still a "delicate balancing act on both sides" between government and the private sector when it comes to sharing this information. Agencies, for example, try to share critical information with the private sector without giving away their methods of obtaining that information.

Meanwhile, agencies recovering from cyber threats just want to "get back to business [and] focus on the mission of their company," Springer said.

"A lot of cyber incidents are taken care of quietly … and so there is a fear that once you get the government involved, that just brings up the profile of everything and increases the likelihood of a lot of media attention or other attention to what is, in reality, a small problem that has already been remedied."


FEDERAL NEWS NETWORK
EXPERT EDITION
SECURITY STRATEGIES IN GOVERNMENT
BROUGHT TO YOU BY:
ANOMALI