Facing near-constant attacks from hackers, nation states and other adversaries, the target sign on the federal government has never been bigger than it is today. Whether physical or virtual, agencies are struggling to stay one step ahead of emerging threat vectors, ensuring systems, data and employees stay safe.

Lightning-speed advances in technology have made the effort to safeguard agency data a constant battle. The challenge lies not only in identifying the newest, vulnerable areas but understanding the attackers’ methods and techniques. Fortunately, agencies are also seeing success leveraging technology in new ways to combat these threats.

This eBook explores the threat landscape for five different areas—defense, energy, finance, mobility and citizen data—across the federal sphere. These areas highlight the need for increased awareness, a willingness to deploy innovative and creative solutions—and swift action.
An unnamed manufacturing firm vital to the U.S. economy recently suffered a prolonged hack, the Department of Homeland Security has disclosed.

The event was complicated by the fact that the company had undergone corporate acquisitions, which introduced more network connections, and consequently a wider attack surface. The firm had more than 100 entry and exit points to the Internet.

The case contains a lesson for civilian and military agencies, both of which are in the early stages of new initiatives to consolidate network entryways.

The breach was reported in a newly released quarterly newsletter from the DHS Industrial Control Systems Cyber Emergency Response Team, which stated the “large critical manufacturing organization was compromised by multiple sophisticated threat actors over a period of several months.”

The victimized organization is “a conglomeration of multiple companies” purchased in recent years, DHS offi-
AGENCIES, CRITICAL INFRASTRUCTURE UNDER ATTACK

Nextgov | Defense

Officials said. The deals required merging multiple networks, which impeded visibility into systems, and “allowed lateral movement from intruders to go largely undetected.”

The manufacturing firm brought in DHS to assist with recovery efforts.

A Homeland Security incident response team probed the business’ networks and found many machines had been breached. It is unclear whether the systems controlled industrial operations or were back-end business systems. The hackers ultimately obtained “privileged access” throughout the network, officials said.

Going forward, “rearchitecting the network is the best approach to ensure that the company has a consistent security posture across its wide enterprise,” officials advised.

AGENCIES TRYING TO HEAD OFF SIMILAR VULNERABILITIES

Federal agencies are attempting to preempt the need for similar overhauls.

Departments are required to limit connections during the development of new IT systems, including Web-based systems. A longstanding governmentwide effort known as “trusted Internet connections,” or TIC, aims to cut the number of external access points to agency networks.

But the cloud has opened up federal systems to untold new Internet connections.

Now, a certification program for Web-based services called the Federal Risk and Authorization Management Program is incorporating the TIC approach from the get-go. FedRAMP and DHS are developing guidelines for agencies that will ensure cloud connections comply with TIC before applications go live, DHS officials announced in September.

Separately, the Pentagon this week announced the Defense Information Systems Agency, Army and Air Force switched on a San Antonio joint regional security stack to move toward “a consolidated, collaborative, and secure Joint Information Environment (JIE) across the Department of Defense.”

The San Antonio base is the first of 25 unclassified data sites that will host firewall protections, intrusion detection systems and other network security functions. Installation is complete at 10 stack sites inside the United States.

David Stickley, who leads JIE implementation, said in a statement the San Antonio upgrade “allows DISA, Army and Air Force to monitor compliance and apply consistent security policy to information traveling over DOD networks.” Other military services are expected to set up similar infrastructures.}

REARCHITECTING THE NETWORK IS THE BEST APPROACH TO ENSURE THAT THE COMPANY HAS A CONSISTENT SECURITY POSTURE ACROSS ITS WIDE ENTERPRISE.  
DHS officials
After 12 years of fighting in the mountains on the Pakistan border and the fields of Helmand province, the United States is planning to withdraw from Afghanistan, ending America’s longest war. But that doesn’t mean the fighting is over.

U.S. forces first entered Afghanistan to find and capture Osama bin Laden on Oct. 7, 2001—just weeks after the Sept. 11 attacks—and disrupt al Qaeda’s most important safe haven. It began as the “good war” with little controversy and a small number of troops with a specific mission. Then the Iraq war diverted American attention, resources and fighting power, dividing the nation as nearly 4,500 American troops were killed and 32,000 wounded. When that war ended in 2010 and President Obama vowed to end the war in Afghanistan, Americans turned their attention elsewhere.

But if there was ever a time to pay attention, it’s now.

BREAKER TK
This final year of the war in Afghanistan will be the most crucial. A bilateral security agreement between Washington and Kabul needs to be reached to allow some U.S. and NATO troops to stay behind to train the Afghan army and police and conduct targeted counterterrorism operations. And a presidential election set for April 5, 2014, will decide who replaces the iconic Hamid Karzai, Afghanistan’s strongman since 2002. All while bringing about half of the more than 50,000 U.S. troops home by February.

Today’s advanced cyber threats hide in plain sight amidst your network traffic, making them nearly impossible to defend against. These cyber threats use applications as their infiltration vector, exhibit application-like evasion tactics and they leverage commonly used network applications for exfiltration.

To fight APTs, only Palo Alto Networks gives the Government visibility to all network traffic so that you can find these cyber threats which use common network applications.

The Palo Alto Networks® 2014 Application Usage and Threat Report exposes the intertwined relationship between cyber attacks and applications using live network data collected from over 5,500 networks worldwide. The report shows you:

• Which applications are the most highly targeted
• Which applications are most commonly used to mask malware activity
• Which applications are the most vulnerable
Firms from half of the nation’s 16 key industries, including wastewater and banking, have paid for special technology to join a Department of Homeland Security program that shares classified cyberthreat intelligence, in hopes of protecting society from a catastrophic cyberattack.

Participation in the Enhanced Cybersecurity Services initiative has more than doubled during the past few months.

Through the voluntary program—previously exclusive to defense contractors—cleared Internet service providers feed nonpublic government information about threats into the anti-malware systems of critical sector networks.

As of July, only three industries—energy, communications and defense—were using the service, according to an unfavorable DHS inspector general audit.

Now, befitting National Cybersecurity Awareness Month, Homeland Security officials say the financial, water, chemical, information technology and transportation sectors also are receiving the threat indicators. Just...
two months ago, American Chemistry Council officials said they had never heard of the program. The service has been available since 2013.

DHS MAKES PROGRAM A PRIORITY

“DHS continues to work closely with our public and private sector partners in expanding the Enhanced Cybersecurity Services program to all critical infrastructure sectors that operate the systems we all rely on,” DHS spokesman S.Y. Lee said in an email. “Information sharing is a key part of the Department of Homeland Security’s important mission to create shared situational awareness of malicious cyber activity.”

The sense is that Andy Ozment, assistant secretary for the DHS Office of Cybersecurity and Communications, who took office in April, has made the program a priority.

“Now that he’s had a few months to get settled, you’re seeing some fruits of labor from his team,” said Dan Waddell, director of U.S. government affairs for (ISC)2, a security industry association.

In May, DHS also deployed automation that “is making the data sharing process much more efficient, so as the word spreads, folks are more likely to join now versus when it was a manual process,” he added.

After Congress failed to pass cybersecurity reforms, President Barack Obama in February 2013 took regulatory action to defend critical infrastructure systems against attackers.

Obama issued an executive order to extend the intelligence-sharing program outside the defense sector and create separate, optional cybersecurity controls. The intelligence-sharing service works by blocking certain IP and email addresses, attachments and additional “signatures” of hacker campaigns that National Security Agency staff and other cyber analysts have discovered.

But the added protection comes with a price tag. Companies typically must cover the costs of new equipment and additional security professionals.

“This is not a trivial exercise and requires a significant investment in people, process and technology on the part of the” ISP or critical infrastructure company, Waddell said.

Even though only half of the industries deemed critical by the government have joined, there’s no cause for concern yet, he said.

“Representation by all 16 of the critical infrastructure sectors would be a major milestone and something that DHS should target in 2015,” Waddell said, adding that as the information exchange grows it will likely attract more firms.

WIDER GROWTH COULD DEPEND ON CONGRESS

Information-sharing programs, in general, might not take off until Congress passes liability protections and customer privacy measures, other cyber experts have said.

DHS officials, acknowledging these concerns, say the

THEY OUGHT TO BE COMPELLED TO SHARE THE INFORMATION BECAUSE IT’S A THREAT...TO THE ENTIRE NATION.

former Attorney General Michael Mukasey

Enhanced Cyber Services program protects civil liberties and is not mandatory.

Some former top administration officials argue government should force businesses to be forthcoming to contain disasters.

“I think they ought to be compelled to share the information because it’s a threat, really, to the entire nation,” former Attorney General Michael Mukasey told reporters last week. “If someone can take down a power grid, I want a power company telling me that.”

However, Mukasey, who served in the Bush administration and now represents private industry as a partner at Debevoise & Plimpton, said companies who admit sensitive data has been jeopardized should not be penalized.

“One of the things that’s going to happen, if they are a publicly held company, is that their stock price is going to suffer as a result, and sure as night follows day there are going to be lawsuits filed by lawyers who are going to claim that they should have known,” he said. “So, somebody has got to provide protection if they have to share the information.”

The advantages of the DHS intelligence program could be worth the risks in some instances, Ozment said recently.

“Our general philosophy is any information-sharing legislation has to be done in a way that it protects privacy and civil liberties, and if it offers liability protection, that has to be narrowly targeted liability protection so that we don’t incentivize anything other than the exact behaviors we are trying to incentivize,” he said at an October 9 panel on cybersecurity hosted by Bloomberg.

Even without broader information information-sharing legislation, Ozment said he’s focused on selling industries on the benefits of the concept.

“Rather than waiting for Congress, what I am doing is focusing on raising that potential upside,” he said. “Here are all the benefits you get from sharing information with the government and with each other.”
If a nation state turns out to be responsible for the JPMorgan hack, the government should respond, the nation’s former top law enforcement official said.

A summer cyber strike on the bank’s network exposed the names, addresses and emails of 76 million households and seven small businesses.

Former Attorney General Michael Mukasey said the proper response to the JPMorgan hack by the government, for now, “is to try to find out who did it and why.”

“If it is a nation state, then the government ought to be able to respond because that is a major part of the economy of the United States,” he added. It “doesn’t have to be a cyber response. You can respond in a whole wide variety of ways. If this was an asymmetric attack, then let’s be asymmetric in response.”

It is said the perpetrators might have ties to Russia or another Eastern European country.

“But I don’t know that it was a nation state,” said Mukasey, the former top cop from 2007 to 2009 under
President George W. Bush.

Mukasey was briefing reporters at a dinner, organized by the French-American Foundation, during a two-day closed-door cybercrime conference convening U.S. and European officials, industry members and security experts.

More broadly, Mukasey said the executive branch’s role in policing cyber mischief is to deploy the capabilities of the National Security Agency. He said the private sector must learn to trust the government and share information about hacks they have suffered -- but he stopped short of calling for mandatory disclosures.

“I think what the executive branch can do is protect the country and its infrastructure through the resources of the NSA,” he said.

Mukasey said it is up to companies to inform the government of their system vulnerabilities.

“They are the ones who innovate, not the government, and they are the ones whose innovations need protection,” said Mukasey, who now represents corporate clients as a partner at Debevoise & Plimpton. “So I think their cooperation with the government is something that ought to be in their interest and they will see that.”

JPMorgan Chase Chief Executive Officer Jamie Dimon earlier in the day reportedly said cooperation between authorities and his bank have been good so far in dealing with a mega-data breach, but coordination likely would need to improve as threats advance.

I THINK WHAT THE EXECUTIVE BRANCH CAN DO IS PROTECT THE COUNTRY AND ITS INFRASTRUCTURE THROUGH THE RESOURCES OF THE NSA

Former Attorney General Michael Mukasey
Federal agencies should repurpose the certification route for vetting commercial cloud computing services to also screen popular mobile apps before employees download them, a top Department of Homeland Security official says.

Nearly every day, white hat hackers discover bugs in app code that bad actors can take advantage of to steal sensitive information.

Just last week, researchers from the University of California and the University of Michigan showed how a flaw in the Gmail Android app could expose a user’s login credentials and other personal information.

Agency personnel are often expected to use such commercial apps, along with homegrown tools, to get their work done. But there’s no way to make popular apps available governmentwide because each agency has different security requirements.

Today, the Pentagon certifies apps, such as Kindle, for troops through the Defense Information Services...
Agency. DHS, meanwhile, has made available to all federal employees a collaborative bug-testing tool called CarWash, which takes about three weeks to report back on vulnerabilities.

**OFFICIAL: FOLLOW THE FEDRAMP MODEL**

But the government’s standards body—the National Institute of Standards and Technology—is just starting to form governmentwide “considerations” for vetting apps.

“Understand that the federal landscape is not the same from one department or organization to another,” said Roberta Stempfley, DHS deputy assistant secretary for cybersecurity strategy and emergency communications.

The government needs to find a path through which agencies can share mobile tools and be assured the apps meet their security needs, she said.

“One of the more successful of those is the FedRAMP accreditation path,” Stempfley said.

FedRAMP, which stands for the Federal Risk and Authorization Management Program, is a baseline security standard all government cloud products, such as Amazon Web Services, must meet before employees can log on.

**GOVERNMENT APP STORE SHELVES STILL A LITTLE SPARSE**

Stempfley, speaking at an event last week hosted by Nextgov, said now is the time to begin a FedRAMP for mobile.

“When I look at what we’ve done over the years,” with cloud security, “we’ve had to build enough momentum between different departments and agencies in order to get to that ... point, and it feels like we’re right on the crux of that now with the mobile app certification work,” she said.

The Centers for Disease Control and Prevention has used commercial apps to track polio immunization efforts overseas.

DISA’s new Mobile Applications Store offered 19 apps as of May, including Pandora, Facebook and a crisis support app for service members dealing with sexual assault.

In February, then-Defense Chief Information Officer Teri Takai acknowledged one challenge with supporting mobile warfighters is efficiently vetting apps.

A concept that might stock app store shelves more quickly?

“Instead of having each department do its own certification for mobile applications, we create a joint model that enables all of the departments to express their unique department requirements—and find the common ground,” Stempfley said.  

**NEARLY EVERY DAY, WHITE HAT HACKERS DISCOVER BUGS IN APP CODE THAT BAD ACTORS CAN TAKE ADVANTAGE OF TO STEAL SENSITIVE INFORMATION.**
The Internal Revenue Service estimates it has paid identity thieves $5.2 billion this year, in a situation where counterintuitively, online transactions might have reduced fraud.

According to auditors, crooks were able to claim tax refunds using stolen taxpayer ID information before the tax agency had time to verify their returns against mailed-in employer wage forms.

To detect fraud, the IRS needs data from employers and the Social Security Administration earlier in the tax season—a workflow problem that can be alleviated by requiring employers to file in January and to do so electronically. Today, electronic employer W-2 forms are due by March 31 and paper W-2 forms are due by Feb. 29.

“Most taxpayers entitled to a refund, along with many identity thieves attempting refund fraud, file early in the filing season—many in February,” a Government Accountability Office report released Mon-
day stated. “During return processing, IRS performs some compliance checks and issues refunds, but at this time it cannot verify the W-2 information for all returns (paper W-2s can be forged and fictitious wage information can be entered on a tax return).”

Currently, only employers filing large amounts of W-2 forms—more than 250—must e-file. GAO recommended lowering that threshold to require employers with at least five to 10 forms also e-file.

“Having more e-filed W-2s would speed processing time for SSA (as compared to paper W-2 processing time) and would enable IRS to receive a larger percentage of W-2 data earlier,” the report states.

The Treasury Department has proposed changing the deadline for all W-2 forms to Jan. 31.

Just one minor obstacle: The gridlocked Congress would have to change the law requiring more employers e-file.

**THIS PROBLEM ISN’T GOING AWAY, UNLESS WE GO HARD AFTER THESE CRIMINALS WHILE ALSO DOING WHAT WE CAN TO PREVENT THIS CRIME**

Some Republicans lay much of the responsibility for hemorrhaging money on the IRS.

“The American people should be able to trust the IRS to protect their identities, preserve their privacy and ensure their hard-earned money isn’t being carelessly flushed down the drain,” Senate Finance Committee Ranking Member Sen. Orrin Hatch, R-Utah, said in a statement. “Sadly, that’s not the case. I hope the IRS will take a serious look at these recommendations and work with Congress to implement smart safeguards.”

Key Democrats seem open to passing reforms to implement the recommendations.

“This problem isn’t going away, unless we go hard after these criminals while also doing what we can to prevent this crime,” Sen. Bill Nelson, D-Fl., said in a statement. “The time has come for Congress to act.”

Finance Committee Chairman Ron Wyden, D-Ore., pledged he would work with other lawmakers and the IRS “to fight this serious and growing problem.”
Aliya Sternstein reports on cybersecurity and homeland security systems. She’s covered technology for more than a decade at such publications as National Journal’s Technology Daily, Federal Computer Week and Forbes. Before joining Government Executive, Sternstein covered agriculture and derivatives trading for Congressional Quarterly. She’s been a guest commentator on C-SPAN, MSNBC, WAMU and Federal News Radio. Sternstein is a graduate of the University of Pennsylvania.