when an automated tabulation method was used to organize that year's Census data encoded on punch cards.

Let me remind our colleagues that we are about to venture on to Census now. Imagine a cyberattack on that process.

Since a modest beginning in 1890, the Federal Government has blazed a path for adoption of computing technology throughout the Federal Government, which established an unprecedented pace for innovation in the private sector that transformed our world from analog to digital in 129 years.

One of the consequences of the Federal Government's use of computing technology over the last 129 years is the challenges of operating legacy systems that use outdated software, which cannot be quickly upgraded to eliminate known cybersecurity vulnerabilities.

Federal Government offices are vulnerable to cyberattacks, with the number of cyber incidents reported by Federal agencies increasing more than 1,300 percent between 2006 and 2015.

In 2015, a hacker exploited access by a government agency contractor to break into the government databases to gain access to 22 million security clearance files from the Office of Personnel Management.

In 2017, Federal agencies reported more than 35,000 cyber incidents, some of which targeted old operating systems that were no longer supported by a vendor.

According to the National Security Agency, it has not responded to a zero-day attack on government systems in the last 4 years because hackers have found better success through basic attack methods.

I would hope my colleagues would consider recognizing that we must be in front of these potential attacks and not behind them.

Mr. Speaker, I reserve the balance of my time.

Mr. GREEN of Tennessee. Mr. Speaker, I urge adoption to the bill, and I yield back the balance of my time.

Ms. JACKSON LEE. Mr. Speaker, I want to thank the minority for its support of this legislation and ask my colleagues to support it.

As I do so, Mr. Speaker, I include in the RECORD an article, "DHS Flags Cybersecurity Vulnerabilities in Philips Patient Monitors: The Department of Homeland Security has issued an advisory about cybersecurity vulnerabilities in the wireless local area network modules of Philips IntelliVue portable patient monitors."

[Sept. 13, 2019]

DHS FLAGS CYBERSECURITY VULNERABILITIES IN PHILIPS PATIENT MONITORS

THE DEPARTMENT OF HOMELAND SECURITY HAS ISSUED AN ADVISORY ABOUT CYBERSECURITY VULNERABILITIES IN THE WIRELESS LOCAL AREA NETWORK MODULES OF PHILIPS INTELLIVUE PORTABLE PATIENT MONITORS

(By Fred Donovan)

The Department of Homeland Security has issued (https://www.us-cert.gov/ics/advisories/ icsma-19-255-01) an advisory about cybersecurity vulnerabilities in the wireless local area network (WLAN) modules of certain Philips IntelliVue portable patient monitors.

DHS's Industrial Control Systems Cyber Emergency Response Team (ICS–CERT) warned that an attacker could corrupt the IntelliVue WLAN firmware and alter the data flow over to the patient monitor, causing an inoperative condition alert at the device and central station.

The vulnerable patient monitors are IntelliVue MP monitors MP20–MP90, MP5/ 5SC, MP2/X2, and MX800/700/600.

The vulnerabilities include use of hard-coded password and download of code without integrity check.

The use of a hard-coded password makes it easier for an attacker to guess the password and login via FTP and upload malicious firmware. In addition, the "product downloads source code or an executable from a remote location and executes the code without sufficiently verifying the origin and integrity of the code," warned the advisory.

Shawn Loveric of Finite State reported the vulnerabilities to Philips.

In a product security advisory (https:// www.usa.philips.com/healthcare/about/cus- tomer-support/product-security), Philips recommended that users of the affected IntelliVue patient monitors update to the WLAN Module Version C wireless module with current firmware.

Philips said it will also issue a software patch for WLAN Version A that will be available by the end of 2019, while WLAN Version B is obsolete.

"Wireless network access should be controlled by authentication and authorization (e.g. WPA2), which are supported by Philips. Additional mitigations include implementing a firewall rule on the customer wireless network, and further controls on physical access to the system," Philips advised.

Philips said it had received no reports of patient harm. Its analysis judged that it is unlikely that the cybersecurity vulnerability would impact clinical use, due to mitigating controls in place. To date, Philips has received no complaints involving clinical use that it has been able to associate with the vulnerability or evidence of patient identifiers compromised.

DHS's Cybersecurity and Infrastructure Security Agency recommended users of the vulnerable Philips devices take defensive measures to minimize the risk of exploitation of these vulnerabilities. Users should restrict system access to authorized personnel and follow a least privilege approach, apply defense-in-depth strategies, and disable unnecessary accounts and services.

Ms. JACKSON LEE. With that in mind, this is a real-life example of what can happen if we are not first in front.

Mr. Speaker, I hope that my colleagues will join me in voting for H.R. 3710, and I yield back the balance of my time.

The SPEAKER pro tempore. The question is on the motion offered by the gentlewoman from Texas (Ms. JACKSON LEE) that the House suspend the rules and pass the bill, H.R. 3710.

The question was taken; and (two-thirds being in the affirmative) the rules were suspended and the bill was passed.

A motion to reconsider was laid on the table.

UNIFYING DHS INTELLIGENCE ENTERPRISE ACT

Ms. JACKSON LEE. Mr. Speaker, I move to suspend the rules and pass the bill (H.R. 2589) to amend the Homeland Security Act of 2002 to establish a homeland intelligence doctrine for the Department of Homeland Security, and for other purposes, as amended.

The Clerk read the title of the bill.

The text of the bill is as follows:

H.R. 2589

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the "Unifying DHS Intelligence Enterprise Act".

SEC. 2. HOMELAND INTELLIGENCE DOCTRINE.

(a) IN GENERAL.—Subtitle A of title II of the Homeland Security Act of 2002 (6 U.S.C. 121 et seq.) is amended by adding at the end the following new section:

"SEC. 210H. HOMELAND INTELLIGENCE DOCTRINE.

"(a) IN GENERAL.—Not later than 180 days after the date of the enactment of this section, the Secretary, acting through the Chief Intelligence Officer of the Department, in coordination with intelligence components of the Department, the Office of the General Counsel, the Privacy Office, and the Office for Civil Rights and Civil Liberties, shall develop and disseminate written Department-wide guidance for the processing, analysis, production, and dissemination of homeland security information (as such term is defined in section 892) and terrorism information (as such term is defined in section 1016 of the Intelligence Reform and Terrorism Prevention Act of 2004 (6 U.S.C. 485)).

"(b) CONTENTS.—The guidance required under subsection (a) shall, at a minimum, include the following:

"(1) A description of guiding principles and purposes of the Department's intelligence enterprise.

"(2) A summary of the roles, responsibilities, and programs of each intelligence component of the Department in the processing, analysis, production, or dissemination of homeland security information and terrorism information, including relevant authorities and restrictions applicable to each such intelligence component.

"(3) Guidance for the processing, analysis, and production of such information.

"(4) Guidance for the dissemination of such information, including within the Department, among and between Federal departments and agencies, among and between State, local, Tribal, and territorial governments, including law enforcement, and with foreign partners and the private sector, consistent with the protection of privacy, civil rights, and civil liberties.

"(5) A description of how the dissemination to the intelligence community (as such term is defined in section 3(4) of the National Security Act of 1947 (50 U.S.C. 3003(4))) and Federal law enforcement of such information assists such entities in carrying out their respective missions.

"(c) FORM.—The guidance required under subsection (a) shall be submitted in unclassified form, but may include a classified annex.

"(d) ANNUAL REVIEW.—For each of the five fiscal years beginning with the first fiscal year that begins after the date of the enactment of this section, the Secretary shall conduct a review of the guidance required under subsection (a) and, as appropriate, revise such guidance.".

(b) CLERICAL AMENDMENT.—The table of contents in section 1(b) of the Homeland Security Act of 2002 is amended by inserting

after the item relating to section 210G the following new item:

"Sec. 210H. Homeland intelligence doctrine.".

SEC. 3. COMPTROLLER GENERAL ASSESSMENT.

(a) ANNUAL ASSESSMENT REQUIRED.—Not later than one year after the date of the enactment of this Act and again not later than five years thereafter, the Comptroller General of the United States shall submit to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate an assessment of the degree to which guidance established pursuant to section 210H of the Homeland Security Act of 2002 (as added by section 2 of this Act) is implemented across the Department of Homeland Security. Such assessment should evaluate the extent to which such guidance is carried out in a manner that protects privacy, civil rights, and civil liberties.

(b) ELEMENTS OF ASSESSMENT.—In conducting each assessment under subsection (a), the Comptroller General of the United States shall—

(1) use standard methodology and reporting formats in order to demonstrate and display any changes over time; and

(2) include any other subject matter the Comptroller General determines appropriate.

(c) ACCESS TO RELEVANT DATA.—To carry out this section, the Secretary of Homeland Security shall ensure that the Comptroller General of the United States has access to all relevant data.

SEC. 4. ANALYSTS FOR THE CHIEF INTELLIGENCE OFFICER.

Paragraph (1) of section 201(e) of the Homeland Security Act of 2002 (6 U.S.C. 121(e)) is amended by adding at the end the following new sentence: "The Secretary shall also provide the Chief Intelligence Officer with a staff having appropriate expertise and experience to assist the Chief Intelligence Officer.".

The SPEAKER pro tempore. Pursuant to the rule, the gentlewoman from Texas (Ms. JACKSON LEE) and the gentleman from Tennessee (Mr. GREEN) each will control 20 minutes.

The Chair recognizes the gentlewoman from Texas.

GENERAL LEAVE

Ms. JACKSON LEE. Mr. Speaker, I ask unanimous consent that all Members may have 5 legislative days to revise and extend their remarks and to include extraneous material on this measure.

The SPEAKER pro tempore. Is there objection to the request of the gentlewoman from Texas?

There was no objection.

Ms. JACKSON LEE. Mr. Speaker, I yield myself such time as I may consume.

Mr. Speaker, I rise today in support of H.R. 2589, the Unifying DHS Intelligence Enterprise Act.

H.R. 2589 seeks to improve the Department of Homeland Security's intelligence enterprise by ensuring intelligence officers across DHS are sharing information and countering threats in a unified manner.

Since the Department was established, intelligence and information sharing capabilities have matured, but DHS still lacks a coordinated intelligence enterprise.

In 2016, the Committee on Homeland Security released a comprehensive re-

view of the Department of Homeland Security's use of intelligence to counter terrorist threats and prescribed 30 recommendations.

As a result, this bill directs the Secretary of Homeland Security, through a DHS chief intelligence officer, to develop and disseminate written DHS-wide guidance for the processing, analysis, production, and dissemination of Homeland Security and terrorism information, and ensures this guidance is consistent with the protection of privacy, civil rights, and civil liberties.

Given the diversity of missions across the Department, it is vital that component intelligence officers are working together, sharing information, and vetting that information against the broader U.S. intelligence community holdings.

H.R. 2589 requires an assessment and description of how the dissemination of information to the intelligence community and Federal law enforcement assists such entities in carrying out their respective missions.

One of the key missions of DHS is to act as a clearinghouse for threat information, and this bill will ensure that the Department continues to evolve into a better, more effective asset in responding to threats to the homeland.

Mr. Speaker, I urge my colleagues to support H.R. 2589, and I reserve the balance of my time.

Mr. GREEN of Tennessee. Mr. Speaker, I yield myself such time as I may consume.

Mr. Speaker, I rise today in support of H.R. 2589, the Unifying DHS Intelligence Enterprise Act.

In December of 2003, I had the unbelievable opportunity to fly with our Nation's elite special operations aviation unit, the Night Stalkers, in conjunction with our Army's tier I counterterrorism unit in the capture of Iraqi dictator Saddam Hussein. It was the highlight of my Army career.

Whether it was on missions in Iraq or hunting Osama bin Laden in Afghanistan, I realized that having a systematic way to gather, process, analyze, and disseminate intelligence information was critical to our success on the battlefield. That experience encouraged me to introduce this bill back in May so that DHS can best fulfill its very important mission to keep America safe.

This bill requires the Department's chief intelligence officer, or CINT, to establish a homeland intelligence doctrine for the Department, and it requires the CINT to maintain a dedicated staff.

In the years following the terrorist attacks of September 11, the Department was established to consolidate 22 existing Federal agencies and reshape the domestic intelligence and counterterrorism structure of the U.S.

Over the years, DHS has matured and refined its intelligence enterprise. Significant improvements have been made, but there is not yet complete unity among the various intelligence

offices within all the component agencies.

In 2016, the House Committee on Homeland Security released a comprehensive review of the Department's use of intelligence to counter terrorist attacks. They recognized that DHS, "has improved its ability to protect the homeland against terrorist threats over time, but major gaps remain." They prescribed over 30 recommendations to the Department for improved intelligence sharing.

The goal of H.R. 2589 is to ensure all of the component entities at DHS are speaking the same language, using the same trade craft, and disseminating their products to the appropriate stakeholders, which include both intelligence communities and State and local partners. This legislation will help professionalize the DHS intelligence enterprise by establishing a shared intelligence doctrine.

Across DHS, dedicated border and immigration agents are gathering information on individuals seeking to enter the United States. Threats to transportation systems and critical infrastructure are gathered and assessed, and real-time cyber threats to the government and private networks are analyzed.

The incredible differences in the agencies of the Department create natural barriers to information flow. Given this diversity of missions, it is vital that component intelligence offices are working together, sharing information, and vetting that information against intelligence community holdings.

As a former member of the Army special operations task forces, I know the value of synchronized intelligence processes in order to connect the dots and successfully carry out a mission. This bill also authorizes the continued dedication to providing staff to the chief intelligence officer ensuring that this distinct mission continues to provide the value necessary to support the intelligence enterprise.

I support this legislation, and I urge my colleagues to join me in doing so.

Mr. Speaker, I reserve the balance of my time.

Ms. JACKSON LEE. Mr. Speaker, I yield myself such time as I may consume.

Mr. Speaker, I thank the gentleman from Tennessee (Mr. GREEN) for his service, and I thank him for this legislation.

It is worth noting that the bill that we just passed and the bill that we are now debating specifically dealing with cybersecurity and intelligence are crucial elements of our security.

I think that with the combination of recognizing the importance of the intelligence community that is on the front lines of providing our safety and then acknowledging the vulnerabilities in the cyber system as one of the components of new technology, I started out my remarks by taking note of the drone attack on the refineries in Saudi

Arabia. Here we are talking about cyber and its impact.

But I think the overall sense of these two initiatives is to ensure that we in Homeland Security are on the front end of dealing with the importance of securing this Nation on the new technologies that we are facing every single day.

I ask my colleagues to support the underlying legislation.

I include in the RECORD the following articles on this very topic: ''Thousands of Vulnerabilities in Seattle's IT Network Attributed to Siloed Approach to Cybersecurity,'' September 17, 2019; ''Leader of New NSA Cybersecurity Directorate Outlines Threats, Objectives,'' dated September 5, 2019; and then, August 30, 2019, ''Why Focusing on Threat Hunting May Leave You Vulnerable.''

[September 17, 2019]

THOUSANDS OF VULNERABILITIES IN SEATTLE'S IT NETWORK ATTRIBUTED TO SILOED APPROACH TO CYBERSECURITY

(By David Kroman)

Last May, Seattle's head of information security flagged a problem within the city's technology department: Because of a process breakdown, employees were indicating that they had fixed vulnerabilities in the department's computer network when, in fact, they had not been fixed.

''It has been discovered that there are currently over 21,000 known critical and high vulnerabilities on systems throughout Seattle IT,'' Andrew Whitaker, then the department's chief information security officer, wrote in a May 22 email to technology leadership. ''Tickets have been closed out, claiming to have vulnerabilities remediated, but upon follow-up review they were, with a few exceptions, not remediated.''

The result was that the servers, desktops and applications within the newly consolidated Department of Information Technology—which now handles the vast majority of the city of Seattle's technology functions, from utilities to the fire department—contained open miniportals that could be accessed by would-be hackers.

When left unremediated, vulnerabilities provide possible paths for hackers to plant spyware, ransomware, viruses and other malicious software that can be immensely harmful to an organization, especially one that provides critical services. Cities are often particularly open to an attack and the effect can be devastating, as recent ransom attacks in Baltimore and Atlanta have shown.

Saad Bashir, Seattle's new head of the Department of Information Technology, said in an interview that he believes the vulnerabilities are manageable. He said Seattle is at risk, as are all organizations, but, in general, not abnormally so.

However, Bashir acknowledged the process breakdown was indicative of a broader problem (https://crosscut.com/2017/07/at-city-hall-a-massive-department-is-mired-in-chaos) he has been attempting to address within the organization since taking his position earlier this year. ''What I observed very early was that there was a siloed approach in how cybersecurity was being practiced in the world of IT,'' he said.

Because of a disconnect between teams, Bashir said, some part of the security process would get completed, but would not be properly handed off to the next team. ''If you're not clear, then you may not know whether that particular vulnerability man-

agement work has been completed the way it's supposed to be completed,'' Bashir said.

In an effort to improve the processes within the department, Bashir began a major reorganization of the relatively new department—including his firing of 14 directors and managers (https://crosscut.com/2019/05/seattles-new-it-boss-fires-14-directors-part-organizational-change)—just two days before Whitaker's message. The reorganization was not motivated solely by security weaknesses, he said, but was intended to create a smoother structure that would better catch possible entry points. When asked if the city was safer from an attack since he took over, Bashir said, ''Absolutely.''

Every organization contains some number of vulnerabilities. The trick is to continually identify and address them as they arise—an e-windshield wiper of sorts, where the vulnerabilities are the raindrops.

Experts say hackers are increasingly less likely to gain access through a vulnerability than they are through a phishing expedition. In such cases, a deceiving email message persuades employees to provide passwords or a malware-infected USB drive is left in a parking lot in hopes that someone finds it and plugs it in to their computer.

But addressing vulnerabilities in the city's systems continues to be an important function of its IT department.

''If I were a serious bad guy I'd be looking at the most vulnerable place,'' said Dr. Barbara Endicott-Popovsky, executive director of the Center for Information Assurance & Cybersecurity at the University of Washington. ''I'd be looking at cities and I'd be looking at universities, because they're open and they can't afford the latest and greatest. It's kind of like, 'Open sesame.' ''

Mike Hamilton, founder of CI Security and Seattle's chief information security officer from 2006 to 2013, said there are a number of reasons cities struggle to stay ahead of cyberattacks.

For one, the number of qualified security experts is down across the country, he said. And of those who are on the market, cities can't match the pay of large companies like Amazon or Microsoft.

''The ones that are good are in short supply, which means that local governments cannot compete for those resources,'' he said.

Additionally, cities are responsible for the security of all their departments, each of which may require vastly different things. ''Because government is a federation of agencies, that makes it a little difficult to have policies in place that apply to [for example] the regulated industry of human resources without raising the ire of unions,'' he said.

Hamilton also said the biennial budgeting of local government makes keeping up challenging. ''Technology moves a whole lot freaking faster,'' he said.

All of this, Hamilton said, is in the context of extremely high stakes. Compared with for-profit companies, ''the potential impact [of an attack on government] is so much greater and government can't afford it,'' said Hamilton. ''We know something needs to be fixed, and we don't fix it until something blows up.''

Bashir said the new processes he's put into place has made him ''confident that we no longer have any glaring process gaps.'' He couldn't say exactly how many vulnerabilities are still open on city systems, but that it was less than 21,000. The ideal number, Bashir said, is zero, but that's also extremely unlikely, which makes it hard to identify what a ''good'' number is.

''I worry about all of them,'' said Andrew Cushman, the city's new chief security officer. ''Whether that number is 21,000 or

whether that number is 10 depends on the attacker and how skilled that attacker is and how motivated that attacker is. So I don't worry more because that number is 21,000, then I do if that number is 10.''

Going forward, Bashir said he wants ''to create a high level of security awareness mindset across the organization.'' The city could have zero vulnerabilities and it wouldn't matter if one employee plugs in the wrong USB to a work computer.

Hamilton said there are several easy things cities can do that, while not offering total protection, would make it so they are no longer ''the slowest gnu in the herd getting picked off.'' For one, mandate zero personal use of city equipment, something Singapore implemented in 2017.

Phishing attacks remain the easiest entry point for hackers and so that's where the bulk of the city's attention should focus, Hamilton said. Because no matter how many protections are put into place, ''There is not now, nor will there ever be, a firewall for stupid.''

———

[From CSO Online, Sept. 5, 2019]

LEADER OF NEW NSA CYBERSECURITY DIRECTORATE OUTLINES THREATS, OBJECTIVES

(By Cynthia Brumfield)

Ransomware, Russia, China, Iran and North Korea are the top cybersecurity threats that will be the focus of a new division within the National Security Agency (NSA), the Cybersecurity Directorate, which is set to be operational on October 1, according to NSA director of cybersecurity Anne Neuberger. She was tapped in July by Director General Paul Nakasone to head the group. The Directorate aims to bring the agency's foreign intelligence and cyber operations together and ''operationalize [its] threat intelligence, vulnerability assessments and cyber defense expertise,'' the agency announced when launching the new division.

''NSA really had to up its game,'' Neuberger said in a fireside chat with Niloofar Razi Howe, cybersecurity venture investor and executive at the Billington Cybersecurity Summit in Washington on September 4. ''And that's what drove this desire to stand up a directorate and frankly to set a pretty aggressive mission, which is to prevent and eradicate cyber actors from national security systems and critical infrastructure with a focus on the defense industrial base.''

In terms of the threats, ''Clearly ransomware is the focus. We've seen there are roughly 4,000 ransomware attacks a day,'' Neuberger said. ''When we look at Russia, we see a country that uses influence operations, uses cyber [that is] really integrated and below the level of armed conflict. They also use entities who aren't necessarily tied to the government, whether the Internet Research Agency for potential elections influence or China has its own unique approach to how the country uses cyber threats to achieve its national security and military objectives, Neuberger said. China's cyber threats are exemplified by three different and wholly distinct types of operations: the 2015 theft of 21.5 million records from the Office of Personnel Management, the hacking campaign known as Cloud Hopper that targeted eight of the world's biggest technology service providers, and ongoing theft of intellectual property such as when Chinese intelligence and business insiders sought to steal information related to a turbofan engine used in commercial airliners.

Iran is very volatile and uses destructive attacks in its own region primarily, Neuberger said. ''North Korea always fascinates us as essentially a nation-state

criminal, as a country under sanctions using creative ways of cyber, whether it's crypto currency, whether it's cryptomining to gain hard currency and essentially keep the regime afloat.''

Neuberger previously headed the agency's "Russia Small Group," a joint NSA-Cyber Command task force to combat Russian election interference and influence campaigns. The task force "was stood up out of a realization that something had dramatically changed and we had to reboot our approach as a US government," Neuberger said.

"Now influence operations have been around since the days of Adam and Eve, but what really changed was the age of social media," she said. Not only could an adversary send out broad messaging, but it could also target disinformation to particular ethnic groups, particular elements of a country, and do it in a "pretty cheap way ... looking as if one is an American.''

"So, we realized that it took a more creative approach to protect our democracy. In the Russia Small Group, we worked closely with the DHS and FBI to ensure that from a cyber perspective they had all the threat information we had in a way that can be quickly actionable'' Neuberger said. "We're tremendously proud of the work we did between NSA, Cyber Command, DHS and the FBI to defend the integrity of our elections and ensure that every American know that their vote counted and their vote matters.,'' referring to the Russia Small Group's efforts to protect the 2018 midterm elections.

When it comes to warding off 2020 election threats, the Directorate will take the same approach the Russia Small Group applied in the 2018 elections. "Ensure there is threat intelligence, gain those insights, share that intelligence, and be prepared to impose costs on an adversary who may attempt to influence our elections," Neuberger said. "We will do the same work that we did in 2018 looking to see who are the actors seeking to shake confidence in the integrity of our elections, and share that with the FBI.''

Ransomware has emerged as a bigger threat to the election infrastructure than it has before. The recent shift ransomware attackers have taken from targeting individuals to targeting entities is "certainly something that would make it be a key concern for the elections. The best protection is the same security advice we give: ensure one uses principles of least privilege [and] computers with admin access shouldn't have access to the Internet at all times.''

Partnering with other government agencies and private sector companies and organizations will be a major focus of the Directorate. "Everything we do, we do in partnership with other agencies, with allies around the world and certainly the private sector plays a role," Neuberger said, noting that she wants to unify all the various communities involved in cybersecurity to enhance collaboration and focus on the hardest cybersecurity problems.

"Partners are key; they are the root of everything we can accomplish," she said. Among the partners the Directorate plans to include in its efforts are the Department of Defense, Cyber Command, DHS, the acquisition community, U.S. allies and certainly the private sector. "The private sector is often the first indicator of a significant threat or a significant compromise.''

The goal is to push out as much unclassified information as possible and bring together all the elements that are needed to quickly identify and head off threats. "Ideally, we are sharing the threat information to prevent an attack, to prevent exploitation rather than being part of a team that helps with incident response," Neuberger said.

Although the Directorate doesn't have a "moonshot" objective as it begins oper-

ations, one goal is to address the "rampant abuse of Internet infrastructure," Neuberger said, particularly protecting the Domain Name System (DNS), the naming system underlying the Internet which has been subject to increasing attacks and redirections by malicious actors.

"DNS is a key way that adversaries use for command and control for exploitation," she said. Neuberger would like to see efforts such as the UK's NCSC's Protective Domain Name System, which was built to thwart the use of DNS for malware distribution and operation, more widely used. The Directorate can help by adding or contributing threat information to make those services even more effective.

The Directorate can serve to interconnect these efforts so they could communicate beyond internet transactions. "If we could achieve that, it would have even broader impact beyond cybersecurity.''

———

[From Infosecurity Magazine] Aug. 30, 2019
WHY FOCUSING ON THREAT HUNTING MAY LEAVE YOU VULNERABLE
(By Bob Shaker)

The cybersecurity threat landscape is becoming increasingly complex and crowded, and with security teams around the world largely understaffed and facing burnout, experts are looking for the most efficient way to combat cybercrime.

One approach that has gained significant momentum of late is threat hunting—the proactive searching of threat indicators within an environment to sniff out highly advanced cyber threats. In threat hunting, security analysts search their environment for known indicators of compromise (IoCs) and adversary tactics, techniques, and procedures (TTPs)—if any of these are found, there's a good chance that an attack is underway.

While threat hunting is a key element of a robust cybersecurity strategy, many organizations rely too heavily on this approach. A narrow focus on specific IoCs and TTPs paints an incomplete picture of the threat environment and means that the attacks that don't bear these hallmarks will get missed.

In this evolving threat landscape, enterprises can't just rely on threat hunting to keep their environments secure—they must broaden their cybersecurity approach, assessing security environments in a more holistic way to better detect advanced and stealth attacks.

WHY THREAT HUNTING HAS BECOME SO POPULAR

Threat hunting has recently become a major buzzword in the security industry in large part because it connotes a cooler, more technical and more skilled approach to security. As a result, security experts are gravitating toward it for career-building opportunities and advancing their security approach.

While threat hunting might be overhyped, there are also genuine benefits to the practice (when done correctly) that help explain why enterprises are so ready to adopt it. Threat hunting helps refocus security teams on emerging threats, since existing security technologies tend to address things we already know about.

Actively looking for emerging threats can mean identifying threats that might be lurking in the environment—reducing dwell time and tackling threats before they escalate and turn into full-blown security breaches.

In addition, adopting threat hunting tactics often leads to discovering visibility gaps in your current security approach—for example, your S3 buckets might not be configured properly or perhaps some firewall rules got changed, or maybe you're able to identify an

employee or group within your organization that is violating a security policy. Uncovering these poorly managed security solutions is a useful byproduct of threat hunting.

THE DOWNFALLS OF THREAT HUNTING

However, many organizations rely too heavily on threat hunting as they are unable to invest in the required infrastructure, resources and expertise to continually analyze all activity for possible threats. Often, this threat hunting is provided by third-party security companies, as many enterprises either lack the skills and resources entirely or are only able dedicate their in-house teams to a few days of threat hunting a year.

With the major talent gap facing cybersecurity, most enterprises simply cannot find or afford to hire professionals with the required level of expertise. As a result, many are turning to managed services offered by security companies to help close the gap. According to Gartner, by 2024, 25% of organizations will be using MDR services, up from less than 5% today.

Threat hunting services often focus almost exclusively on threats posed by splashy, sexy attack groups—whether it is notable criminal APTs or nation state groups. A strong security program focuses on risk management, and one of the most important things security teams can do is accurately identify the risks that they are susceptible to, which for many enterprises isn't a nation-state attack.

While threat-hunting addresses attacks that everyone is talking about, the reality is that many enterprises should be equally—if not more cognizant—of commodity threats. While sophisticated threats exist and are important to defend against through threat hunting, the majority of threats facing enterprises are better addressed through good security hygiene.

Over-investing in threat hunting can lead to an incomplete and irregular picture of the risks enterprises face. In fact, a singular reliance on threat hunting alone means that many types of attacks will get missed if you're not specifically looking for them.

TAKING A HOLISTIC APPROACH

By over-rotating on big name threats, security teams leave open the possibility that they are going to miss the obvious. In this threat environment, security teams can't afford to drop the ball on the basics—a recent ESG survey of enterprise cybersecurity leaders revealed that more than three-quarters (76%) believe that threat detection and incident response is more difficult today than it was just two years ago.

To ensure a strong security posture, enterprises should take a comprehensive, multifaceted approach that goes beyond threat hunting. As they build out a holistic approach, they should be sure to:

Collect data on everything they can. Often when investigating a breach or incident, security teams find that they don't have any evidence because they aren't collecting and retaining the right data—it's usually the exception when there's sufficient logging for an incident. With living off the land attacks increasing (many of which fly under the radar of traditional logging), it's ever more important that teams don't skimp on data collection, as relying on a mixture of sources is more likely to help you detect threats early and prevent bad actors from getting in unnoticed.

Use multiple security tools and strategies. We've recently seen a trend toward new technologies like AI and machine learning across security programs. It's important to layer these tools and strategies as they each have their strengths and weaknesses. To maximize effectiveness, use a mixture of tools, methodologies and frameworks that integrate multiple attack and adversary considerations such as MITRE ATT&CK as well as

simple IOCs, rule-based detection, statistical models, linguistic models, and machine learning models—and then correlate with global threat intelligence, validating and augmenting with human expertise.

Don't underestimate the importance of humans. The human side of the investigation is critical. There is no better computer for detecting, recognizing and responding to threats than the human mind. While automated systems have helped advance the security industry significantly, a true "eyes on glass" approach to threat detection requires years of experience and the corresponding intuition of knowing when something is amiss.

Ms. JACKSON LEE. Mr. Speaker, I ask that my colleagues support the underlying legislation, and I reserve the balance of my time.

Mr. GREEN of Tennessee. Mr. Speaker, there is bipartisan support for a professional, coordinated Department of Homeland Security intelligence architecture.

I want to thank Chairman THOMPSON and Ranking Member ROGERS for supporting this legislation and bringing it to the floor. It is time for DHS to be able to function with the same precision in the handling of intelligence information as our warriors in the Department of Defense, and I am honored to have the opportunity to help them do so.

Mr. Speaker, I urge support of the bill, and I yield back the balance of my time.

Ms. JACKSON LEE. Mr. Speaker, I ask my colleagues to support the underlying bill, and I yield back the balance of my time.

The SPEAKER pro tempore. The question is on the motion offered by the gentlewoman from Texas (Ms. JACKSON LEE) that the House suspend the rules and pass the bill, H.R. 2589, as amended.

The question was taken; and (two-thirds being in the affirmative) the rules were suspended and the bill, as amended, was passed.

A motion to reconsider was laid on the table.

_____

MESSAGE FROM THE SENATE

A message from the Senate by Ms. Byrd, one of its clerks, announced that the Senate has passed without amendment a bill of the House of the following title:

H.R. 4378. An act making continuing appropriations for fiscal year 2020, and for other purposes.

_____

□ 1400

TSA REACHING ACROSS NATIONALITIES, SOCIETIES, AND LANGUAGES TO ADVANCE TRAVELER EDUCATION ACT

Mr. CORREA. Mr. Speaker, I move to suspend the rules and pass the bill (H.R. 3691) to require the TSA to develop a plan to ensure that TSA material disseminated in major airports can be better understood by more people accessing such airports, and for other purposes.

The Clerk read the title of the bill.
The text of the bill is as follows:

H.R. 3691

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the "TSA Reaching Across Nationalities, Societies, and Languages to Advance Traveler Education Act" or the "TRANSLATE Act".

SEC. 2. PLAN.

(a) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act, the Administrator of the Transportation Security Administration (TSA) shall submit to the Committee on Homeland Security of the House of Representatives and the Committee on Commerce, Science, and Transportation of the Senate a plan to ensure that TSA material disseminated in major airports can be better understood by more people accessing such airports.

(b) CONTENTS.—The plan required under subsection (a) shall include the following:

(1) An identification of the most common languages other than English that are the primary languages of individuals that travel through or work in each major airport.

(2) A plan to improve—

(A) TSA materials to communicate information in languages identified pursuant to paragraph (1); and

(B) the communication of TSA material to individuals with vision or hearing impairments or other possible barriers to understanding such material.

(c) CONSIDERATIONS.—In developing the plan required under subsection (a), the Administrator of the TSA, acting through the Office of Civil Rights and Liberties, Ombudsman and Traveler Engagement of the TSA, shall take into consideration data regarding the following:

(1) International enplanement.

(2) Local populations surrounding major airports.

(d) IMPLEMENTATION.—Not later than 180 days after the submission of the plan required under subsection (a), the Administrator of the TSA shall implement such plan.

(e) GAO REVIEW.—Not later than one year after the implementation pursuant to subsection (d) of the plan required under subsection (a), the Comptroller General of the United States shall submit to the Committee on Homeland Security of the House of Representatives and the Committee on Commerce, Science, and Transportation of the Senate a review of such implementation.

(f) DEFINITIONS.—In this section:

(1) AIRPORT.—The term "airport" has the meaning given such term in section 40102 of title 49, United States Code.

(2) MAJOR AIRPORTS.—The term "major airports" means Category X and Category I airports.

(3) TSA MATERIAL.—The term "TSA material" means signs, videos, audio messages, websites, press releases, social media postings, and other communications published and disseminated by the Administrator of the TSA in Category X and Category I airports.

The SPEAKER pro tempore (Mr. CUELLAR). Pursuant to the rule, the gentleman from California (Mr. CORREA) and the gentleman from Tennessee (Mr. GREEN) each will control 20 minutes.

The Chair recognizes the gentleman from California.

GENERAL LEAVE

Mr. CORREA. Mr. Speaker, I ask unanimous consent that all Members may have 5 legislative days to revise and extend their remarks and to include extraneous materials on this measure.

The SPEAKER pro tempore. Is there objection to the request of the gentleman from California?

There was no objection.

Mr. CORREA. Mr. Speaker, I yield myself such time as I may consume.

Mr. Speaker, I rise today in strong support of H.R. 3691, the TRANSLATE Act.

Throughout my travels, I get the opportunity to witness and meet families and visitors from numerous countries, cultures, and backgrounds traveling throughout our Nation's airports.

These families share many of the same experiences we all share when traveling using an airplane. They want to board their flights on time and land safely at their destination without undue delay or confusion.

Sadly, signs and other communications throughout our U.S. airports are not meeting the needs of all travelers. Many non-English speakers, international travelers, and people with vision or hearing impairments experience challenges during their travels because the current signage is not accessible to them.

According to the U.S. Census, over 65 million individuals living in the U.S. over the age of five speak English not well or not at all.

No one should have to worry about missing a flight because they don't speak English or have impaired vision or hearing.

This bill addresses this issue by requiring TSA to make signage, video, audio, and other online content more accessible to travelers at major airports who do not speak English as their primary language.

This bill will make TSA operations more effective and efficient by helping to prevent miscommunication between TSA officers and travelers.

Furthermore, this bill helps ensure that we maintain a standard of inclusivity at our airports for residents and visitors alike.

Mr. Speaker, I urge my House colleagues to support this legislation, and I reserve the balance of my time.

Mr. GREEN of Tennessee. Mr. Speaker, I yield myself as much time as I may consume.

Mr. Speaker, I rise today in support of H.R. 3691, the TRANSLATE Act. TSA has an important mission to protect air travel and is responsible for the security of nearly 440 Federalized airports. Across these airports, TSA screens more than 2 million passengers a day.

To accomplish this mission, TSA relies on materials like signs, websites, and videos to communicate screening information to passengers and airport employees prior to their arrival at TSA checkpoints.

H.R. 3691 requires TSA to develop and implement a plan to identify languages other than English that are primary