COMBATING RANSOMWARE ATTACKS

JOINT HEARING

BEFORE THE

SUBCOMMITTEE ON CYBERSECURITY, INFORMATION TECHNOLOGY, AND GOVERNMENT INNOVATION

AND THE

SUBCOMMITTEE ON ECONOMIC GROWTH, ENERGY POLICY, AND REGULATORY AFFAIRS

OF THE

COMMITTEE ON OVERSIGHT AND ACCOUNTABILITY

HOUSE OF REPRESENTATIVES

ONE HUNDRED EIGHTEENTH CONGRESS

FIRST SESSION

SEPTEMBER 27, 2023

Serial No. 118–68

Printed for the use of the Committee on Oversight and Accountability

Available on: *govinfo.gov*
oversight.house.gov or
docs.house.gov

U.S. GOVERNMENT PUBLISHING OFFICE
53–719 PDF WASHINGTON : 2023

COMMITTEE ON OVERSIGHT AND ACCOUNTABILITY

JAMES COMER, Kentucky, Chairman

JIM JORDAN, Ohio
MIKE TURNER, Ohio
PAUL GOSAR, Arizona
VIRGINIA FOXX, North Carolina
GLENN GROTHMAN, Wisconsin
GARY PALMER, Alabama
CLAY HIGGINS, Louisiana
PETE SESSIONS, Texas
ANDY BIGGS, Arizona
NANCY MACE, South Carolina
JAKE LATURNER, Kansas
PAT FALLON, Texas
BYRON DONALDS, Florida
KELLY ARMSTRONG, North Dakota
SCOTT PERRY, Pennsylvania
WILLIAM TIMMONS, South Carolina
TIM BURCHETT, Tennessee
MARJORIE TAYLOR GREENE, Georgia
LISA MCCLAIN, Michigan
LAUREN BOEBERT, Colorado
RUSSELL FRY, South Carolina
ANNA PAULINA LUNA, Florida
CHUCK EDWARDS, North Carolina
NICK LANGWORTHY, New York
ERIC BURLISON, Missouri

JAMIE RASKIN, Maryland, *Ranking Minority Member*
ELEANOR HOLMES NORTON, District of Columbia
STEPHEN F. LYNCH, Massachusetts
GERALD E. CONNOLLY, Virginia
RAJA KRISHNAMOORTHI, Illinois
RO KHANNA, California
KWEISI MFUME, Maryland
ALEXANDRIA OCASIO-CORTEZ, New York
KATIE PORTER, California
CORI BUSH, Missouri
JIMMY GOMEZ, California
SHONTEL BROWN, Ohio
MELANIE STANSBURY, New Mexico
ROBERT GARCIA, California
MAXWELL FROST, Florida
SUMMER LEE, Pennsylvania
GREG CASAR, Texas
JASMINE CROCKETT, Texas
DAN GOLDMAN, New York
JARED MOSKOWITZ, Florida
RASHIDA TLAIB, Michigan

MARK MARIN, Staff Director
JESSICA DONLON, Deputy Staff Director and General Counsel
RAJ BHARWANI, Senior Professional Staff Member
LAUREN LOMBARDO, Senior Policy Analyst
PETER WARREN, Senior Advisor
JEANNE KUEHL, Senior Professional Staff Member
MALLORY COGAR, Deputy Director of Operations and Chief Clerk

CONTACT NUMBER: 202-225-5074

JULIE TAGEN, Minority Staff Director

CONTACT NUMBER: 202-225-5051

SUBCOMMITTEE ON CYBERSECURITY, INFORMATION TECHNOLOGY, AND GOVERNMENT INNOVATION

NANCY MACE, South Carolina, Chairwoman

WILLIAM TIMMONS, South Carolina
TIM BURCHETT, Tennessee
MARJORIE TAYLOR GREENE, Georgia
ANNA PAULINA LUNA, Florida
CHUCK EDWARDS, North Carolina
NICK LANGWORTHY, New York
ERIC BURLISON, Missouri
Vacancy

GERALD E. CONNOLLY, Virginia *Ranking Minority Member*
RO KHANNA, California
STEPHEN F. LYNCH, Massachusetts
KWEISI MFUME, Maryland
JIMMY GOMEZ, California
JARED MOSKOWITZ, Florida
Vacancy

SUBCOMMITTEE ON ECONOMIC GROWTH, ENERGY POLICY, AND REGULATORY AFFAIRS

PAT FALLON, Texas, Chairman

BYRON DONALDS, Florida
SCOTT PERRY, Pennsylvania
LISA MCCLAIN, Michigan
LAUREN BOEBERT, Colorado
RUSSELL FRY, South Carolina
ANNA PAULINA LUNA, Florida
CHUCK EDWARDS, North Carolina
NICK LANGWORTHY, New York

CORI BUSH, Missouri, *Ranking Minority Member*
SHONTEL BROWN, Ohio
MELANIE STANSBURY, New Mexico
ELEANOR HOLMES NORTON, District of Columbia
RAJA KRISHNAMOORTHI, Illinois
RO KHANNA, California
Vacancy

C O N T E N T S

WITNESSES

Written opening statements and statements for the witnesses are available on the U.S. House of Representatives Document Repository at: docs.house.gov.

INDEX OF DOCUMENTS

Documents are available at: docs.house.gov.

COMBATING RANSOMWARE ATTACKS

Wednesday, September 27, 2023

HOUSE OF REPRESENTATIVES
COMMITTEE ON OVERSIGHT AND ACCOUNTABILITY
SUBCOMMITTEE ON CYBERSECURITY, INFORMATION TECHNOLOGY, AND GOVERNMENT INNOVATION
AND THE
SUBCOMMITTEE ON ECONOMIC GROWTH, ENERGY POLICY, AND REGULATORY AFFAIRS
Washington, D.C.

The Subcommittee met, pursuant to notice, at 1:03 p.m., in room 2154, Rayburn House Office Building, Hon. Nancy Mace [Chairwoman of the Subcommittee on Cybersecurity, Information Technology, and Government Innovation] presiding.

Present from the Subcommittee on Cybersecurity, Information Technology, and Government Innovation: Representatives Mace, Timmons, Burchett, Edwards, Langworthy, Connolly, and Lynch.

Present from the Subcommittee on Economic Growth, Energy Policy, and Regulatory Affairs: Representatives Fallon, Fry, Brown, and Norton.

Ms. MACE. Good afternoon, everyone, and welcome. This is a joint hearing of two Subcommittees of the Committee on Oversight and Accountability. One is a Subcommittee I chair, the Subcommittee on Cybersecurity, Information Technology, and Government Innovation. The other is a Subcommittee on Economic Growth, Energy Policy, and Regulatory Affairs, which is chaired by my esteemed colleague from Texas, Mr. Fallon. Since this is a joint hearing, we will have opening statements from the Chair and Ranking Member of both Subcommittees. That is a total of four opening statements, so I will attempt to keep mine brief.

Cybersecurity has been a major focus of ours. Since I became the Subcommittee Chair, I am concerned that we, as a Nation, are not prepared for the increasingly sophisticated cyberattacks that will be fueled by AI. Businesses and government entities in my district and across the country have faced cyberattacks and been forced to pay huge sums of money in ransoms. The Federal Government itself still stores a sensitive data of tens of millions of Americans on half-century-old legacy systems running on COBOL, of all languages, which I learned at the age of 21, over 20 years ago, a coding language decades older than myself and Chairman Fallon. And

we have got a shortage across the country of 700,000 cybersecurity professionals with job vacancies strewn across the public and private sector. We need all hands on deck to fill the gap. That is why I have sponsored legislation eliminating unnecessary degree hurdles to Federal cybersecurity jobs. The government cannot be turning away people with much-needed cyber skills just because they lack a 4-year degree.

Cyberattacks come in different forms, but today we are focusing on ransomware attacks. These are intended to deny users access to files or entire computer systems. The perpetrators pledge to restore access if a ransom is paid and often charge an additional ransom for not disclosing sensitive stolen data. These sorts of attacks are nothing new. They have existed for decades, but back then they were unsophisticated and often unsuccessful in locking down systems. Amateur hackers were trying to squeeze small ransoms from individual users. The field has now matured and grown. That became clear in May 2021 when the hackers, likely based in Russia or Eastern Europe, brought one of the major gas pipelines in this country to a standstill. The Colonial Pipeline went entirely offline briefly, causing the Federal Department of Transportation to declare an emergency in 17 states and here in D.C. in order to keep fuel supply lines open.

In fact, when that hack happened was when we saw in the Southeast and in my home state of South Carolina, that is when gas prices really started to increase, and then they just never went back down. The problem shows no signs of going away. Malicious actors are constantly searching for areas of vulnerability. At the height of COVID, truly demented actors' favorite targets, like hospitals and schools, even the ransomware supply chain has expanded. Hackers now offer ransomware as a service to other criminal enterprises.

The bottom line is that it is too easy today for malicious actors to do too much damage and make too much money with too few consequences. So, we need to engage in this fight at all levels. Schools, hospitals, and businesses cannot fight a battle alone against adversaries launching attacks from enemy nation-states like Russia and China and elsewhere. It is going to take effective partnerships, including with Federal law enforcement, and that includes figuring out how to better collect and share information about these attacks and the attackers.

As we will hear today, the institutions victimized by ransomware have options, but all of them are bad. They either pay ransom or they are unable to restore their normal operations. Attackers threaten to release sensitive personal data that has been stolen. In the case of schools and hospitals, that includes school children's education records and patient medical records. We will hear today from representatives of a school and a hospital victimized by ransomware attacks. We will also hear from a cybersecurity expert whose current work includes counseling companies that are targets and victims of these attacks.

I hope this hearing today will help educate us on the problem and that it will serve as a step toward better addressing it. With that, I yield to the Ranking Member of this Subcommittee, Mr. Connolly.

Mr. CONNOLLY. Thank you, Madam Chairwoman. Thank you for having this hearing. Welcome to our witnesses.

Though we are discussing the threats of ransomware, we cannot ignore the much greater danger caused by some, a government shutdown. The Cybersecurity and Infrastructure Security Agency, for example, will be forced to furlough more than 80 percent of its workforce.

As we say, we are concerned about cyber hacking and cyberthreats. Without funding, our crucial Federal cyber defenses will be reduced to a skeleton crew and yet still hold responsibilities to respond to attacks in our networks and critical infrastructure. We cannot allow this to happen when we already know of the innumerable malware attacks constantly threatening our economy, schools, public health, critical infrastructure, and national security.

Ransomware is a burgeoning multibillion dollar criminal industry. In 2021, the estimated cost of ransomware damage globally hovered around $20 billion. This year, that number is $30 billion, a 50-percent increase in just 2 years. The United States is a major target. Between January and December 2022, known ransomware attacks on public and private networks in the United States increased by 47 percent. More troubling, these tallies include only those incidents victims report.

While the recent MGM Resorts International hack received considerable public attention, these kinds of ransomware attacks also target critical infrastructure. In 2021, for example, the U.S. Government had to declare a regional emergency, as you noted, Madam Chairwoman, after the Colonial Pipeline was taken down, the largest fuel pipeline system in the country. That incident was just one frightening reminder of what is at stake. State and local governments are particularly vulnerable because they are responsible for storing much of our personally identifiable information, but they lack the cybersecurity resources and protections and funding as billion dollar conglomerates. Criminals also do not discriminate between large metro areas and small towns. Communities of all sizes have been victims, including Dallas, Texas; Oakland, California; and Lowell, Massachusetts.

A 2023 ransomware report from Sophos found that nearly 70 percent of the surveyed IT leaders in state and local governments reported ransomware attacks. Just as troubling, the report found that educational systems are the most likely to be targeted.

I ask unanimous consent, Madam Chair, to insert this report into the hearing record.

Ms. MACE. Without objection.

Mr. CONNOLLY. I thank the Chair. I know this firsthand from when a ransomware attack in 2020 targeted the Fairfax County Public School system, the 10th largest school system in America, which I represent.

Members of this Committee are well aware of how the coronavirus pandemic abruptly revealed how ill-prepared many of our state and local governments were in delivering vital public services securely and remotely through their IT platforms. Criminals took advantage of that in unemployment systems, in direct checks payments to families and small business loans, and on and on.

That is why during my tenure as Chairman of the Government Operations Subcommittee, which included this Subcommittee, we held hearings on the outdated IT infrastructure and rising cyberattacks on state and local governments. The hearing examined the role of Congress and the Federal Government in accelerating IT modernization initiatives. In response to the hearing, we introduced House companion to the Senate's State and Local Digital Service Act. This important legislation provided guidance and, critically, funding for state and local governments to form digital service teams focused on delivering fair, effective, and secure public services. I certainly hope this Congress will continue that work.

Furthermore, we helped to champion the Bipartisan Infrastructure Bill, providing more than a billion dollars in vital investments to assist both public and private entities who fall victim to cyberattacks every year. Earlier this year, the Biden-Harris Administration also published its National Cybersecurity Strategy, which addresses these, among other issues, head on by laying out an action plan to disrupt ransomware criminals. It lays out four key pillars to disrupt them by, one, leveraging international cooperation to disrupt their ransomware ecosystem and isolate those countries that provide safe havens; two, investigating ransomware crimes and using law enforcement and other authorities to disrupt it and them; and third, bolstering critical infrastructure resilience to withstand such attacks; and fourth, addressing the abuse of virtual currency to launder ransom payments.

The Department of Justice also continues to hold ransomware criminals accountable, and most recently dismantling the Qakbot or CrackBot network and seizing more than $8.6 million in cryptocurrency profits. That is great, but it is a modest start. While these are important first steps, much more has to be done, and I know we are going to hear that from our witnesses today. I look forward to hearing the testimony and working with you, Madam Chairwoman and Mr. Fallon and others, and, of course, Ms. Brown, in trying to craft thoughtful solutions to deter and ultimately prevent ransomware attacks, and I thank you. I yield back.

Ms. MACE. Thank you. I will now recognize Chairman Fallon for the purpose of making your opening statement.

Mr. FALLON. Thank you, Chairwoman Mace, and I want to thank everybody for being here today as well. I am grateful that the EER Subcommittee and Subcommittee on Cybersecurity are teaming up to talk about a very important problem.

America relies on technology, of course, every day, and when you rely on something, when it goes down, you become very vulnerable when it is gone, but, you know, it has a far-reaching consequences when it is jeopardized. While ransomware attacks our digital files and hold, you know, data hostage until ransom is paid, the true cost of cyberattacks go well beyond simply the money surrendered to perpetrators. Frozen systems wreak havoc on normal operating procedures of a company, a school, a hospital, and forcing reallocation of staff, lost revenue, and damaged reputations.

Following an attack, institutions may have to completely re-outfit their entire IT infrastructure, very costly, and scrambling to redirect funds earmarked for other investments, or more investment, say, in personnel. Mountain Dew could get, you know, in a

cyberattack, and then where would our colleague from Tennessee be? But, you know, you might be making investments in teachers and other personnel. I mean, it is our most valuable natural resource, but that is going to be preventing new hires and make you more efficient because you have to deal with these ransomware attacks, and Congress should be very concerned about these attacks and where they are originating from. The vast majority are coming from Russia, a country that clearly does not have our best interests at heart.

When these sorts of attacks target essential sectors, like the electric grid or the hospital system, what we saw with Colonial Pipeline or JBS a couple of years ago, they endanger public health, safety, and, quite frankly, put American lives at risk. And we saw that they can even have impacts that spiral well beyond the original attack into the larger economy, again, with Colonial Pipeline, that reverberated, and it was very dangerous and very chilling.

As our world becomes more reliant on technology, unfortunately, the opportunities for bad actors to use that technology for their own monetary and political gain become more and more abundant. But no matter what the size of the attack, we must prevent hackers from being able to use ransomware to upend American institutions and risk our Nation's prosperity and health and American lives. I am grateful for our witnesses who are here today to share their stories and help us examine the ongoing threat of ransomware attacks. And during this hearing, I hope to explore the role of government in helping prevent further attacks and punishing those that would go after our critical infrastructures. Whether the government is providing resources for private organizations undergoing attacks or learning how to better protect our own systems, I look forward to discussing potential ways Congress can enable the Cybersecurity and Infrastructure Security Agency, or CISA, the FBI, and other Federal agencies to better protect the American people and our data. Thank you, Madam Chair, and I yield back.

Ms. MACE. Thank you. I would now like to recognize Congresswoman Brown for the purposes of an opening statement.

Ms. BROWN. Thank you, Madam Chair Mace, Mr. Chair Fallon, and Ranking Member Connolly, and thank you to the witnesses for joining us today.

Our hearing today addresses an issue threatening Americans far too frequently: ransomware attacks. Criminals, both foreign and domestic, use ransomware to target everything and everyone: private businesses, state and local governments, hospitals, school districts, and critical infrastructure. We have seen these attacks disrupt access to primary healthcare and safety net services for our Nation's most vulnerable.

But before I go any further, we cannot sit at this hearing without addressing the terrible dangers we face with an impending Republican Government shutdown. A government shutdown, much like a ransomware attack, would be dangerous, destructive, and disastrous. The Cybersecurity and Infrastructure Security Agency, the Agency that leads Federal cybersecurity efforts and serves as the national coordinator for critical infrastructure security and resilience, would have to furlough 80 percent of its employees as a re-

sult of the Republican shutdown. We are talking thousands of critical workers, people with families, and that is just one agency. The Department of Justice, the Agency responsible for investigating and taking down criminal ransomware networks, would also be forced to furlough thousands of employees. With a shutdown, extreme Republican members would undercut organizations and state and local governments relying on Federal funds to prevent the crippling ransomware attacks we are discussing in this very hearing.

All over the country, ransomware attacks directly affect people's lives. Hospitals have to turn away patients. Nine-eleven call centers would have been unable to dispatch ambulances and fire trucks. Small businesses have to close down. In some instances, people have been unable to pay their water bills because a city website had been paralyzed by a hacker demanding ransom, and those late fees, they add up. In my home state, ransomware thieves targeted the Ohio unemployment system in July, preventing thousands of Ohioans from receiving benefits. And in March, the Lakeland Community College in Ohio, just next door to my district, was the victim of a cyberattack that compromised the personal data of nearly 3,000 individuals.

Now, the Biden-Harris Administration has made defending against these kinds of attacks a top priority. Thanks to the Bipartisan Infrastructure Bill, the Administration is currently providing $1 billion in cybersecurity grants to state, local, and territory governments to build the cyber capabilities they need. But on Sunday at 12:01 a.m., these dollars are at risk of not making it out at all. It is just one more reason the MAGA shutdown is harmful to everyday people, our national security, and our standing in the world. And with that, Madam Chair, I yield back.

Ms. MACE. Thank you. I am pleased to introduce our witnesses for today's hearing. Our first witness is Mr. Grant Schneider, Senior Director of Cybersecurity Services at Venable. Our second witness is Dr. Lacey Gosch, Assistant Superintendent of Technology at Judson Independent School District. Our third witness is Dr. Stephen Leffler, President and Chief Operating Officer of the University of Vermont Medical Center. And our last witness today is Mr. Sam Rubin, Vice President and Global Head of Operations at Palo Alto Networks Unit 42. Welcome, everyone. We are pleased to have you this afternoon.

Pursuant to Committee Rule 9(g), the witnesses will please stand and raise their right hands. All right.

Do you solemnly swear or affirm that the testimony you are about to give is the truth, the whole truth, and nothing but the truth, so help you God?

[A chorus of ayes.]

Ms. MACE. Let the record show the witnesses all answered in the affirmative. Thank you.

We appreciate all of you for being here today and look forward to your testimony. Let me remind the witnesses that we have read your written statements, and they will appear in full in the hearing record.

Please limit your oral introductory statements to 5 minutes. As a reminder, please press the button on the microphone in front of you so that it is on, and Members can hear you. When you begin

to speak, the light in front of you will turn green. After 4 minutes, the light will turn yellow. When the red light comes on, your 5 minutes has expired, and we would ask you to please wrap it up.

So, I will first recognize Mr. Schneider to please begin your opening statement.

STATEMENT OF GRANT SCHNEIDER
SENIOR DIRECTOR OF CYBERSECURITY SERVICES
VENABLE, LLP

Mr. SCHNEIDER. Thank you very much. Chairwoman Mace, Chairman Fallon, Ranking Member Connolly, Ranking Member Bush, Members of the Committee and your staff, thank you for the privilege to appear before you today.

I have spent my entire 30-year career focused on our Nation's security. This includes over 20 years at the Defense Intelligence Agency, 7 of which I served as the Chief Information Officer and 6 years at the Executive Office of the President, serving as a Senior Director for Cybersecurity Policy on the National Security Council staff, and most recently as the Federal Chief Information Security Officer. For the past 3 years, I have been a Senior Director of Cybersecurity Services at Venable, a law firm, where I help our clients, both large and small from all sectors, enhance their cybersecurity programs through the development and implementation of risk management strategies.

Between my time in government and at Venable, I have supported numerous organizations with the preparation, response, and recovery from various cyber incidents, including ransomware attacks. Some of these include leading the response and recovery for a regional healthcare delivery organization that was the victim of ransomware, creating playbooks and decision matrices to help clients consider the actions they may need to take in the event of a significant incident, and working with law enforcement, CISA, and the intelligence community and other interagency partners on ways to disrupt malicious cyber actors.

I want to thank the Committees for taking up the important issues related to ransomware. As has been mentioned, ransomware is a form of cyberattack where a malicious actor typically steals sensitive information, encrypts a victim's files and systems, and then demands a payment, a ransom, in order to return services to operation. To be clear, ransomware is a means for malicious actors to make money. It is rarely about foreign policy or espionage objectives like those we see from nation-state actors. However, policy discussions are complicated by the fact that many ransomware actors are protected and sometimes endorsed and encouraged by the nations from which they operate.

While malicious cyber activity and ransomware have been around for decades, several factors, which have been mentioned, have come together in recent years to expand the frequency, scale, and public awareness of ransomware events. Organizations today are dependent on technology to develop and deliver their services. This includes organization and education, healthcare delivery, financial services, energy, and every other critical infrastructure sector. These enhancements provide increased productivity, convenience, and broad delivery of services to customers. At the same

time, more critical services and sensitive data have moved to an internet-accessible environment and are at risk.

Concurrently, ransomware actors have increased access to malicious tools, anonymous payment systems, and safe havens from which to operate. Government organizations have published alerts and guides to help educate private organizations and individuals on defensive cybersecurity controls they can put in place. Some of these include implementing phishing-resistant multi-factor authentication to protect users' digital identity, a robust set of system backup and recovery tools and procedures, encryption of data at rest and in transit, and training for employees to recognize phishing emails and social engineering attempts.

Policymakers cannot lose sight of the fact that ransomware has devastating operational, economic, and reputational impacts on its victim organizations. During a ransomware event, government organizations, including law enforcement, can provide a very limited amount of support. Victims are left with an unsavory set of options, having to choose between restoring services quickly by paying a ransom or working to reconstitute their systems and restore operations on their own. Often, paying a ransom can be the most time- and cost-effective approach to getting an organization up and running again. Given these dynamics for victims, ransomware remains a prevalent threat to large and small businesses, public sector entities, and critical infrastructure organizations. In short, it is bad, but there is hope.

The United States and international partners have invested heavily in disrupting ransomware activities across the globe, including the takedown of the Hive ransomware group earlier this year. Cybersecurity experts have partnered with policy professionals to propose legal and policy updates that will empower law enforcement officials and other cyber defenders to pursue these malicious actors and build resilience across our digital ecosystem. We must continue to develop these ideas while working with companies and public sector entities to harden their networks and protect their data.

Thank you again for the opportunity to speak with you today, and I look forward to your questions.

Ms. MACE. Thank you, Mr. Schneider. I will now recognize Dr. Gosch for her opening statement.

STATEMENT OF LACEY GOSCH
ASSISTANT SUPERINTENDENT OF TECHNOLOGY
JUDSON INDEPENDENT SCHOOL DISTRICT

Ms. GOSCH. Thank you, Chairwoman Mace, Chairman Fallon, Ranking Member Connolly, Ranking Member Bush, Committee Members, and staff, for allowing me to speak with you today. I represent the Judson Independent School District as the Assistant Superintendent of Technology, and I am here to share our experience with ransomware. My primary professional role and the events related to the testimony are from my experience as the leader of the technology department serving over 24,000 students and 4,500 employees across seven municipalities in the San Antonio, Texas area. I also serve as an elected school board member for the Navarro

Independent School District. Therefore, my passion for seeking school support and combating cybercrime runs very deep.

On June 17, 2021, I received a call from Matthew Fields stating that our system had been affected by ransomware. He briefly investigated the depth of the attack and confirmed the ransom note's content. The ransom note stated that all data on all devices and all servers was encrypted, including our backup systems. We immediately contacted law enforcement and Federal Bureau of Investigations. The threat actors were identified as PYSA, a variant of the Mespinoza strain of malware, commonly leveraged in high-paying assaults and victim selections based on their ability to pay. In 2021, PYSA was the third most prevalent ransomware strain with primary targets of higher education and K–12 schools. The group was most notably known for their double extortion involving publicizing stolen information should victims refuse to comply with their demands.

The attack initiated from a single vector with two pivot points. The entry vector and first pivot point was one of my employee's computers. The second pivot point was a video streaming server that was designed to have no outside connectivity and was used for internal video streaming only. From these points, the threat actors were able to penetrate the backup systems, data stores, and devices connected to the network. From the full investigation, a total of 428,761 individuals were affected, and those individuals are living in all 50 states.

The recovery of our network was not our primary concern. We had ample resources to restore our systems. Our concern was the security of the data by the threat actors and preventing the release of that personally identifiable information of our constituents. Consequently, the district made the difficult decision to pay the negotiated amount of ransom totaling $547,000 on June 29. Our recovery took more than a year, and the district continues to make improvements. The restoration of the network was only possible through the efforts of my technology team's perseverance, key vendor partners, and some school district friends that assisted us in communications and business operation functions when others were too scared to even take our calls. Thankfully, there are companies and school district partners who saw our situation as an opportunity to learn. We learned that the cavalry does not come, and we must rely on our own resources. No state or Federal agency ever visited or offered recovery assistance to us.

Insurance coverage was helpful, but those go predominantly to attorney's fees, data mining, and identity protection. It does not cover ransom payments or cost for upgrades to mitigate that damage. The cost for repair exceeds the limits of the policy, forcing districts to make difficult decisions about funding allocations. And the costs are not limited to data loss or data breach, but they extend to monetary loss and recovery and replacement efforts, security efforts, and mental and physical health effects that are rarely discussed or considered because of these events.

I was hired only 34 days prior to this attack in the school district. The state of the district's technology was not unlike thousands of school districts across the Nation. It was outdated, out of support, and included antiquated systems and hardware that in-

cluded outdated infrastructure that could not support the changes brought about by COVID–19. These factors attributed to our vulnerability and in the continued concern for many K–12 leaders.

Schools are often forced to balance the needs for student curriculum, personnel resources, facilities, and other operations on limited budgets. Therefore, funding for solutions to prevent attacks and protect data and upgrade equipment is pushed aside for more visible and tangible items. Recovery and mitigation programs for cybersecurity have not been formally developed for schools, but we would recommend potentially discount programs similar to things like E-Rate and other federally supported programs. Additionally, there are other measures, such as standards for network security, requirements for making Social Security numbers masked in all systems, training educational programs, and social-emotional programs for affected individuals is also needed.

I would like to thank the Committee today for providing the structure to hear these issues. I am honored to be able to present this information to you and to have you hear our story and recommendations. Thank you, Chairwoman Mace, Chairman Fallon, Ranking Member Connolly, and all the staff involved. I am honored and privileged to be here.

Ms. MACE. Thank you, Dr. Gosch. I would like to recognize Dr. Leffler for his opening statement.

STATEMENT OF STEPHEN LEFFLER
PRESIDENT AND CHIEF OPERATING OFFICER
THE UNIVERSITY OF VERMONT MEDICAL CENTER

Dr. LEFFLER. Thank you. The University of Vermont Medical Center is the tertiary care hospital and academic medical center for the state of Vermont. We are the only one in Vermont. We care both for local patients in Chittenden County, but for all Vermonters across the state who have life-threatening illnesses.

On October 28th of 2020, we were 7 months into the pandemic when we suffered a ransomware cyberattack. We are extremely fortunate that when that attack first started, before our IT team even knew what was occurring, they made the decision to shut down our system. That was a critically important move. They did that before contacting the leaders because they realized something was wrong. That single move protected any patient care information from being released, any employee information being released, and was key to our overall action during the pandemic.

Over the next month, we had two major initiatives. The first one was an IT initiative to restore our network back to normal. The cyberattack, while it did not affect our patient information, did infect 1,300 servers at the University of Vermont Medical Center and 5,000 desktop computers. Every single computer needed to be wiped clean and then reimaged. Every server had to be wiped clean and reimaged. It was a 24-hour-a-day, 7-day-a-week job for our IT staff. We were very fortunate the state of Vermont realized how important this was and gave us National Guard workers to help with that reimaging.

The second major focus for us was patient care. We are the sole tertiary care hospital in our state. We did not have the option of stopping care, shutting down, going on diversion. We knew we

would have to take care of people. The cyberattack impacted our electronic medical records for more than 28 days, and so on day two of the cyberattack, we set up two incident command teams. An IT incident command team focused on restoring our IT systems—there were 600 applications that had to be cleaned and brought back online—and a clinical incident command team that was completely focused on how we provide care on paper.

The extent of the attack was broad. We did not have internet. We did not have phones. It impacted radiology imaging, laboratory results, and because the EMR had been shut off appropriately, we did not have the EMR for 28 days. We were back to paper. For an older doctor like me, paper was pretty familiar, but many of our young new doctors had never written paper orders. We had to go back and teach them how to do that. We brought together our clinical leaders from surgery, anesthesia, trauma, emergency medicine, obstetrics medicine, and they met sometimes twice a day, 7 days a week for 28 days to decide how they could safely provide care for patients who we knew would be showing up, what care could be safely delayed, and what care could be transferred out of state to other academic medical centers who could help us.

Over the course of that month, we delivered hundreds of babies, did trauma surgery. We did heart surgery. We did multiple other cancer staging operations all safely with high quality on paper. We did have to delay care for some patients. We used those extra providers to provide an extra set of eyes and hands to make sure that paper system was working. Over the course of the month that we did not have our EMR, every day we were focused on what needed to come up first and how. A major issue that we faced is that in 2020, best practice was to save 3 days of forward-looking information in your electronic medical record. Our cyberattack happened on a Thursday. On Monday morning, our clinics did not know who were going to show up in the clinic that day, did not have their medical information, did not have their problem list, did not know what time they were coming or for what. I had to go on the news and say if you are coming for an appointment today, bring everything you have with you to help us take care of you.

Early in the cyberattack, the first 2 days, we did not have a phone system because our phone is on the internet. We literally went to Best Buy and bought every walkie-talkie they had, and I asked our administrators all to basically run lab results to the floors. Our critical lab results system was down. On day two, we had a pile of paper lab results in our pathology conference room about 6 inches thick of lab results for our patients. We used our medical students to actually file all those results.

Over the course of our month, we took care of hundreds of patients safely, but it was hard. I have been an emergency medicine doctor for 30 years. I have been the hospital president for 4 years. The cyberattack was much harder than the pandemic by far. Thank you very much.

Ms. MACE. Thank you, and I would now like to recognize Mr. Rubin for your opening statement.

STATEMENT OF SAM RUBIN
VICE PRESIDENT AND GLOBAL HEAD OF OPERATIONS
PALO ALTO NETWORKS– UNIT 42

Mr. RUBIN. Chairs Mace and Fallon, Ranking Member Connolly, and distinguished Members of the Committee, thank you for the opportunity to testify on combating ransomware attacks. My name is Sam Rubin. I am the Vice President of Global Operations at Unit 42, which is Palo Alto Network's Incident Response and Threat Intelligence Division.

For those not familiar with Palo Alto Networks, we are an American-headquartered cybersecurity company founded in 2005 that has since grown to protect tens of thousands of organizations around the world. We support critical infrastructure operators, the U.S. Federal Government, universities and other educational institutions, and a wide range of state and local partners. This means that we have a deep and broad visibility into the cyber threat landscape. We are committed to using this visibility to be good cyber citizens and national security partners with the Federal Government.

We look at our role as a cybersecurity leader with great humility. We envision a world where each day is safer and more secure than the day before, and this takes all of us working together. The current cyber threat landscape demands this posture. My written testimony includes some concerning numbers and trends, many of which we heard here today, and we are seeing the ransomware threat grow as well. Attackers are using increasingly sophisticated methods to extort money. My written testimony also highlights that if we look at our global attack surface through the eyes of the adversary, it looks porous and far too inviting. Entities of all sizes are struggling to understand and manage their digital infrastructure, their computers, their servers, their mobile devices, and all the rest that they have connected to the internet. Despite this sobering backdrop, at Palo Alto Networks, we remain confident that we are well-equipped to combat the cyber incursions of today and tomorrow for several reasons.

First, important advances in technology, especially in artificial intelligence and automation, are absolutely force multipliers in cybersecurity defense. For too long, defenders have been inundated with alerts to triage manually, creating an inefficient game of Whack-a-Mole, while critical alerts go unmissed, and vulnerabilities remain exposed. We sit at a strategic inflection point to flip this paradigm. Second, cybersecurity is increasingly being recognized by entities of all sizes, public and private, as a critically important issue. We need to take the next steps now. Every enterprise must recognize cybersecurity not just as an IT concern, but as a core part of their enterprise risk management strategy. Third, policymakers are showing a sustained desire to support cyber defenders. Thank you for that. As just one example, the State and Local Cybersecurity Grant Program is already showing the potential to increase resilience to ransomware attacks across all corners of the country.

Cybersecurity matters to all of us. Ransomware attacks impact our daily lives, from disruptions to public services like hospitals, to interruptions to supply chains, to critical gas pipelines being taken

offline. My team at Palo Alto Networks specializes in helping organizations respond and recover in their darkest hours when they have been hit by a cyber incident. Our mission goes beyond just recovery. We aim to elevate their cybersecurity posture so when they come out of it, they are stronger than before. That is what makes the work so fulfilling for me personally.

That spirit of partnership in the cybersecurity community, the notion that we are all in this together must remain in our collective DNA. As a company, we are proud to participate in a number of forums like CISA's JCDC, not to sell our products, but to share our situational awareness and our threat intelligence and our understanding of the cyber threat landscape. Critically, in forums like these, commercial competitors become threat intelligence partners. So, I wanted to thank you for the opportunity to testify today, and I look forward to your questions.

Ms. MACE. Thank you, Mr. Rubin. I would now like to recognize myself for 5 minutes, and I have a few questions for everybody. We only have 5 minutes, so I will try to be as quick as possible, and we will just ask for as brief an answer as possible as well. Mr. Rubin, I am going to start with you. AI and cyber criminals, are they using AI to deploy ransomware attacks?

Mr. RUBIN. Thank you, Congresswoman. This is a threat that we are watching very closely at Palo Alto Networks. From a threat intelligence standpoint, we are also doing testing in our own labs to try to recreate some of the potential capabilities. At this point, we are not seeing any new or novel attack techniques generated by AI.

Ms. MACE. Do we have defenses, or what kind of defenses do we have against AI-powered attacks?

Mr. RUBIN. Right. We have the ability to use AI to our benefit to help protect organizations, and that is absolutely what we are doing at Palo Alto Networks is to create capability that leverages AI to protect——

Ms. MACE. For our defenses?

Mr. RUBIN. And for our defenses.

Ms. MACE. And I apologize. I want to run through because I want to ask everybody a few questions, but the Atlanta Fed published an article earlier this year, saying it was 144-percent increase in ransomware from 2020 to 2021. That is massive. Is this across any specific sectors—government, private, large or small, certain industries, or is it spread evenly throughout?

Mr. RUBIN. Yes. From our data and from our threat intelligence from the incident response work we do, we see these primarily as crimes of opportunity where the threat actors are leveraging automated scanning capability to find vulnerabilities, and then attack those organizations that are vulnerable.

Ms. MACE. And then, Mr. Schneider, you know, in this same report, they said that their average ransom payment—I could not believe this—was almost $5 million. And given that the concentration of some of these attackers are in hostile nations, is it safe to assume that some of this money might be used by criminal enterprises, you know, to line the pockets of our adversaries?

Mr. SCHNEIDER. Well, I think all of it is being used by criminal enterprises. And it is, you know, funding and further fueling addi-

tional ransomware investments in AI and other technologies to exacerbate——

Ms. MACE. What country is the worst? Which one of our adversaries is the absolute—leading the world in these kinds of ransom attacks?

Mr. SCHNEIDER. I mean, from the research I have seen, generally Russia is, you know, is a safe haven and a lot of ransomware actors there.

Ms. MACE. Yes. Thank you. And then I have a few questions for Dr. Gosch and Dr. Leffler, although I will just kind of ask them evenly if you can both respond. But, you know, in some cases, ransom is paid, some it is not, but just if you all can sort of generally say—it is not just a ransom fee, if it was paid, that would be the cost of this. There is a much larger cost to an organization, a school, or a hospital. What do you guys estimate cost, when this attack happened, cost the school and/or the hospital?

Ms. GOSCH. I would say from our experience, it was very similar to what was shared from the hospital side in that we had to replace almost everything, upwards of potentially $3 million, $4 million, $5 million.

Ms. MACE. Dr. Leffler?

Dr. LEFFLER. For UVM Medical Center, it was $65 million in cost.

Ms. MACE. Yes, and for $3 million to $5 million for a school, sometimes that is a school's budget, I mean, you know, depending on the size, if it is a local school, et cetera. Do you feel that what you have seen and experienced that you have learned from it, and what kind of steps have you taken that you think other people should be aware of that they should be doing right now to help protect the organization or institution?

Dr. LEFFLER. I am a physician, not an IT expert, but I do understand that we have put things in place since that attack happened. When the bad actors got into our system, they were able to move around at will inside the system. We have added a lot of steps to sub-segment our system into pieces and to make it harder for our administrators to make changes. We have added multifactor authentication to our administrators we did not have before, and I have been assured that will make it much harder when they get in again. We assume it is going to happen again. There are so many people trying.

Ms. MACE. Dr. Gosch?

Ms. GOSCH. We have done similar. We are using AI to monitor all of our email protection systems. We are also using multifactor authentication. We have moved to immutable backups and a lot of technologies that we did not have before. Everything is cloud-based and provides that extra layer of protection, extra password pieces, and other components that had been told an EDR is one of the big pieces, the endpoint protection and recovery. So, we have added those at a high cost, and that is always a concern as we look at school budgets in terms of maintaining it, but we were able to upgrade to what is needed to combat it.

Ms. MACE. And how long did that take?

Ms. GOSCH. We are still working on some of those initiatives now. It took us a full year to get all of our systems back online,

and we continue to make improvements by adding things like port security within our network and additional security measures on the back end on the infrastructure.

Ms. MACE. Thank you so much, and I yield back. I yield to my colleague from Virginia, Mr. Connolly, for 5 minutes.

Mr. CONNOLLY. I thank the Chair, and I want to welcome Mr. Schneider, in particular, who is my neighbor in Mantua in Fairfax County. We live in the same neighborhood, so welcome. And speaking of Mr. Schneider, Mr. Schneider, I begin my opening statement by noting that, should the government shut down, as it almost certainly is going to on Saturday, 80 percent of the employees of CISA will be furloughed. What could go wrong with that?

Mr. SCHNEIDER. Well, certainly, CISA has an extremely significant role for the Nation for cybersecurity, both in working with critical infrastructure, but also for their preparation efforts, but also on being able to get alerts and information along those lines out. I do not know which 20 percent of CISA is going to be retained and what functions. I would hope that they are going to continue to be able to do the operational pieces and put out alerts as they see emerging threats start to evolve.

Mr. CONNOLLY. But I guess we would both agree 20 percent cannot really handle what 100 percent normally handle. Something is going to give, and at the very least, there is a risk.

Mr. SCHNEIDER. Yes.

Mr. CONNOLLY. Yes, in terms of our mission. Thank you. Dr. Leffler, I was really struck by the story of the hospital in Vermont, and I had images. When we were doing healthcare, I did a lot of tours of health centers and hospitals. And, you know, I had in my mind, like, a dialysis unit where you have many, many patients in the round, and you have sort of a central computer screen monitoring their progress. Likewise, in an oncology unit, same thing with chemo. And so, I was particularly thinking, well, those patients and those units are particularly vulnerable if you shut that down in a ransomware attack because you have got 20 or 30 patients at a time often either on dialysis or on chemotherapy. Was your hospital affected with respect to those patients?

Dr. LEFFLER. So, we kept both those units open because those patients needed to stay alive, so dialysis, obviously, people are life dependent on dialysis. We added staff is what we did. We switched to paper. We added more staff members.

Mr. CONNOLLY. So, but the ransomware did affect——

Dr. LEFFLER. It did affect it.

Mr. CONNOLLY. It did affect them.

Dr. LEFFLER. It affected every single part of our function, everything that we do.

Mr. CONNOLLY. Unbelievable. I think that is really important because in addition to the story of schools, and my school system also was attacked, but now we are talking life and death, and the criticality of a hospital cannot be overstated and the vulnerability of hospitals. You said something really profound, "I am not a tech expert. I am a doctor," and we cannot expect everybody in their field of endeavor to be tech experts. And yet, that is the vulnerability, and it affects directly your ability to perform your functions and to serve your patients.

So, Mr. Rubin, I was struck by the fact that you used the term, "We are trying to create a new paradigm," and what strikes me about ransomware is everything about our response is reactionary. The paradigm is entirely defensive. Either you do or you do not pay the ransom, and then after the fact, we try to shore up and buttress our assets and our resources to prevent it from recurring. It seems to me if we are going to have a new paradigm, it has got to be a lot more proactive and preemptive rather than reactive. I would give you the opportunity to comment on that.

Mr. RUBIN. Yes. Thank you, Congressman. I completely agree with you. We need to move the focus into taking steps ahead of time sort of in peace time, so to speak. And organizations, public and private, need to invest in their cybersecurity posture, in their awareness, and in their, essentially, defenses to take steps ahead of time, absolutely.

Mr. CONNOLLY. To what extent would you say that the vulnerability today often reflects, because Dr. Gosch put her finger on it and really resonates with me after the pandemic experience, that an awful lot, especially at state and local levels, you know, we are just not investing in the IT platforms to keep them robust and cyber secure. To what extent do you think that is a big part of the problem?

Mr. RUBIN. I do think that that is a big part of the problem. Investing in cybersecurity is an exercise in economics. It is the allocation of scarce resources. And we heard about operating budgets, and so there is always cost benefit decisions being made about where to put money, and sometimes investing in a cybersecurity resource or tool might mean something else goes unfunded, and so it is hard for state and local organizations. So, that is why I think programs like the State and Local Cybersecurity Grant Program are a phenomenal resource for state and local entities to avail of to try and get some more resources to help themselves out there.

Mr. CONNOLLY. I could not agree with you more, and I think it is an overlooked part of the vulnerability spectrum, and we saw that reflected in pandemic. Take unemployment insurance, vulnerable, 50 different systems, not one, and, you know, lots of vulnerabilities. I yield back. Thank you, Madam Chair.

Ms. MACE. Thank you so much. I would now like to recognize Mr. Fallon from Texas for 5 minutes.

Mr. FALLON. Thank you, Madam Chair. Mr. Schneider, when there is a government shutdown, just to clear something up, it is up to the Administration, is it not, to use exemptions for folks to come into work?

Mr. SCHNEIDER. Yes, there are several exemptions allowed——

Mr. FALLON. Like the Antideficiency Act, there are exemptions authorized by law to protect human life, for protection of property?

Mr. SCHNEIDER. Correct.

Mr. FALLON. OK. So, you would not have to furlough 80 percent of CISA. You could have all of them come into work if you so choose.

Mr. SCHNEIDER. I mean, I do not know what decision CISA is making about——

Mr. FALLON. But it is up to the Administration.

Mr. SCHNEIDER. But it is up to the Administration to——

Mr. FALLON. So, we could have everybody come into work. OK.

Mr. SCHNEIDER [continuing]. To come into work, yes.

Mr. FALLON. I just wanted to point that out. And as far as the shutdown goes, well, we will save that for our close. Dr. Gosch, thank you for making the trip all the way from Texas, the Lone Star state. You know, your school was hit with a ransomware attack, and can you just describe, did you pay the ransom?

Ms. GOSCH. Yes, we did.

Mr. FALLON. OK. And how much did you have to pay?

Ms. GOSCH. Five hundred and forty-seven thousand dollars was the final amount.

Mr. FALLON. Yes. And I think you touched upon this with Chairman Mace, but what were your best and greatest takeaways from the experience as far as preventing it from happening again?

Ms. GOSCH. Our best and greatest takeaway is that it is not a matter of if you are going to be hit by some attack. It is going to be your ability to mitigate and to defend and to recover quickly. In our situation, one of the things that stuck out for us was the need to continually maintain the upgrade and to make sure that the systems are on the back end, and be able to promote that information to other school district leaders because in similar situations, I am supposed to be the tech expert in this, but in many cases, the leaders of the school districts are not the tech experts.

And so, making sure that that message is heard and how important it is to be proactive in the process, and to put in multiple ways in which to monitor. And to utilize—I know AI can be seen as the danger in terms of ransomware, but at the same time, it can also provide so much additional support for identifying a potential threat because there are simply not enough man hours in the day, and there is not enough people to look——

Mr. FALLON. Sure. Sure.

Ms. GOSCH [continuing]. At all the code that is coming in.

Mr. FALLON. Mr. Schneider, just let us say on average, 6 years ago, if a medium-sized company was hit with an attack, what was the usual asking price? What was the ransom?

Mr. SCHNEIDER. So, I was in government at the time. I am not sure I have a great number, but the numbers have certainly increased.

Mr. FALLON. I think Mr. Rubin is going to help us out.

Mr. SCHNEIDER. That would be Mr. Rubin, yes.

Mr. FALLON. Mr. Rubin, go ahead.

Mr. RUBIN. Yes. So, we have seen the numbers grow almost exponentially year over year. So, I think you said 5 or 6 years ago, it was in the, you know, low six figures, if breaking $100,000. And the data varies, but right now, you know, our average from our data was over $650,000, on average.

Mr. FALLON. And that is consistent with—we got the idea after the Colonial Pipeline, JBS, and then when we were appointed to the Subcommittee Chairs, got the idea to have this Committee hearing, I reached out to some business people I know in Texas. And I found it very interesting that the average ask it seems in that neighborhood was about that $50 grand range years ago, and now it is 10 times that, 12 times that, and that is frightening.

And then a lot of people, we say, oh, it is, you know, X amount of attacks. We do not know really how many because there are so many folks that pay and are embarrassed that they paid. A friend of mine, who will remain nameless because I do not want him to be a continued target, he got hit, but he had a backup system that was good enough to where he did not have to pay and he just rolled into that. And then they just worked on, you know, basically securing the wall, if you will, moving forward.

Dr. Leffler, University of Vermont Medical Center was hit in 2020. Is that correct?

Dr. LEFFLER. Yes.

Mr. FALLON. Did you all pay the ransom?

Dr. LEFFLER. We did not pay the ransom. We had a good backup.

Mr. FALLON. But you said, you know, the good backup, but it still cost you $65 million?

Dr. LEFFLER. Sixty-five million dollars.

Mr. FALLON. And where was most of the loss?

Dr. LEFFLER. It was in cleaning and rebooting the system. It was in care that was deferred. It was in extra staff to care for the patients that we cared for. It was across the board.

Mr. FALLON. Well, being originally from Massachusetts, right down Route 7, you know, I feel for you. You know, go Vermont. Mr. Schneider, we have heard from Dr. Leffler and about the impacts with ransomware attacks, I mean, $65 million bucks. Can you explain how cyberattacks on critical infrastructure, like the one we had with Colonial Pipeline in 2021, can affect the industries and communities beyond the victimized operation?

Mr. SCHNEIDER. Yes. Thank you for the question. Certainly, Colonial Pipeline is a great example where the pipeline was shut down. I think by all reporting, it was not actually impacted by the ransomware, but they had to shut it down out of an abundance of caution. And then the ripple effect on the entire East Coast, if you were trying to get any fuel, you could not, there were long lines certainly at gas stations, and that just has a trickle-down effect on, or, you know, exponential impact or broader impact on the economy, writ large.

Mr. FALLON. My time has expired. Thank you, Madam Chair. I yield back.

Ms. MACE. Thank you. I would now like to recognize Congresswoman Brown from Ohio for 5 minutes.

Ms. BROWN. Thank you, Madam Chair. In March of this year, the Biden-Harris Administration released the National Cybersecurity Strategy, a first-of-its kind effort to combat ransomware attacks. This comprehensive government effort prioritizes the protection of our Nation's economy, infrastructure, national security, and public health.

The Administration's sophisticated strategy addresses long-term solutions to cybersecurity challenges, including the need for a workforce prepared to deal with these 21st century issues, like complex, elaborate, and long-running ransomware threats. The next generation of our workforce, those who are in college, trade schools or newly reentering the workforce, are often our first line of defense against cyberattacks. In today's integrated economy, all sectors have critical technology components, which are vulnerable

to ransomware. That is why a prepared workforce is essential to our national response. So, Mr. Rubin, in what ways has the Biden-Harris Administration's National Cybersecurity Strategy expanded educational programs to diversify, grow, and equip the cybersecurity workforce?

Mr. RUBIN. Thank you, Congresswoman. We applaud the new cybersecurity strategy. There is much in there that really aligned with our vision for how to keep organizations safe, enhance visibility, focusing on zero trust, talking about preparedness in IR plans, but with respect to training and educating individuals, there is also a lot there as well, something that Palo Alto Networks supports as well. We have a program that we call the Cybersecurity Academy that provides free curriculum to middle school through college students to help train and bring up the workforce of the future.

Ms. BROWN. Thank you for that. Now, when conducting the hiring initiatives promoted by the Biden-Harris Administration, it is important to highlight the current demographic disparities in the cyber workforce this plan rightly seeks to address. A 2021 report from the Aspen Institute found only 4 percent of cybersecurity workers identify as Hispanic, 9 percent as Black, and 24 percent as women. Mr. Rubin, how can we incentivize hiring a more diverse cyber workforce, and what best practices have you seen to recruit tech talent from communities which are currently underrepresented?

Mr. RUBIN. Thank you, again, Congresswoman. I think, you know, one of Palo Alto Network's core values is inclusion, and we work hard to make sure that we do have diversity in the workforce. And so, I think the first step is awareness and being conscious of this as something that is important, and that we all do better when we have people from different backgrounds and different perspectives. Another program that Palo Alto Networks has is recruiting college graduates into a program we call the Unit 42 Academy. There are college graduates that join our workforce, and I am proud to say that this current class is actually 80 percent female, but that includes, you know, broad diversity as well.

Ms. BROWN. Thank you for that. Additionally, as a Member of the Select Committee on Strategic Competition between the United States and the Chinese Communist Party, I am committed to working with our international partners to protect the United States from malicious foreign cyberattacks. It is extremely disturbing we have terrorist groups as well as nations like Russia, North Korea, and China, working to disrupt our cyber systems and our strategic alliances in the West. So, Mr. Rubin or Mr. Schneider, in what ways can the United States work more closely with our international partners to combat the threat of ransomware attacks and other cybersecurity challenges? Thank you.

Mr. SCHNEIDER. I mean, thank you for the question, ma'am. I think to your point, we have to have this as an international, you know, collaboration in order to put an amount of pressure on ransomware actors and on the nation-states from which they are operating. And there are a variety of tools that can be used for that, whether they are diplomatic tools, but we are going to have to work together in order to make any real progress on this area.

Ms. BROWN. Thank you. Mr. Rubin?

Mr. RUBIN. I agree. I think that I would put them in the categories of disruption and deterrence. On the disruption side, it is leveraging that diplomatic pressure, using carrots and sticks, where we can influence law enforcement action and takedowns, and we have seen some of that more recently, but I think there is a long way to go.

Ms. BROWN. And thank you very much. Clearly, the President's comprehensive cybersecurity plan, which involves everything from an expanded and better trained workforce to cooperation with our international partners, is already paying off. I am ready to work in a bipartisan manner to strengthen and support the President's initiative, and with that Madam Chair, I yield back.

Ms. MACE. Thank you. I would now call on my colleague from Tennessee, Congressman Burchett. Do not screw it up.

Mr. BURCHETT. Thank you, Chairlady. I will try not to. Thank you all for being here. All the good questions have been asked pretty much, but let me ask here down the line, what can we do to fix this?

Mr. SCHNEIDER. Thank you for the question. I think that is the question of the day, right? And it is something that——

Mr. BURCHETT. That is not going to get you anywhere, complimenting me up here. It is better off if you attack me and insult me, and then everybody else will agree with you, but go right ahead.

[Laughter.]

Mr. SCHNEIDER. Well, I probably will not go down that route, sir. We have to approach both from a defensive standpoint and what defensive measures, cybersecurity controls can companies and organization put in place in order to protect their systems, to have good backups of their systems, to encrypt their own data so they cannot be encrypted by someone else and taken from them. And as we were just discussing, we need to be able to disrupt and deter actors in cyberspace, and we really need to find a way to shift the value proposition for ransomware actors. Today, they are able to do this with almost impunity and make a lot of money at it, and we have got to find kind of a whole of government and a whole of working with our allies to make real progress here.

Mr. BURCHETT. Are any of our ally countries have people involved in this? I mean, it always seems like every time we come out and say you are not going to break into this system, then some 12-year-old kid in somebody's garage gets into the system.

Mr. SCHNEIDER. Now, I think we have a really good international cooperation on this. You know, as this hearing notes, it is a really big challenge, and so it does not always feel like we are making the progress——

Mr. BURCHETT. OK.

Mr. SCHNEIDER [continuing]. But I think we are, you know, building those interactions across nations with a lot of our key allies.

Mr. BURCHETT. All right. Doctor, how do you say your last name, ma'am?

Ms. GOSCH. Gosch.

Mr. BURCHETT. Gosch. All right.

Ms. GOSCH. Yes, sir.

Mr. BURCHETT. Good, I am glad. Go ahead.

Ms. GOSCH. So, from the educational standpoint, I think a lot of the things that could help school districts really has to do with funding and some discount programs and things like that, but additionally, there really needs to be some additional standards set for schools. There really is not any governing———

Mr. BURCHETT. Right, because a lot of this equipment is so outdated.

Ms. GOSCH. Correct.

Mr. BURCHETT. I mean, you are sitting here talking to us. I mean, I remember when Mace asked me to be on this Committee, I thought, you know, a bunch of guys up here in powder blue leisure suits still listening to the eight-track tape players in their 1972 AMC Gremlins, you know, I mean, we are the ones going to be making decisions on that, so I can appreciate that.

Ms. GOSCH. And there are other aspects of that. You know, we spend a lot of time on emergency operations plans, but at least in Texas, there are not any particular guidance or requirements to deal with cybersecurity. It is just not talked about within education. It is not something that is supposed to necessarily happen. I know in our case, a lot of times people think that due to lack of backups and things like that is why we went the route that we went, and we had all of the backups. That was not our issue. And then there are a lot of other regulatory things that would help in the cybersecurity piece as far as student data, just in having some regulations even on software companies.

Mr. BURCHETT. Dr. Leffler?

Dr. LEFFLER. I agree with my colleague that from a hospital perspective, a lot of it is funding and grants. So, in every budget that we build, as a doctor, I want to spend all the money on patient care, technology, new equipment there. Prior to the cyberattack, usually cybersecurity stuff would fall down the budget, oftentimes come off. And so, having ways to more cheaply buy programs and have those programs be current and new and upgraded, or grants to bring your hospital up to standards, have a strong backup so you do not have to pay the ransom, would make a huge difference, I believe.

Mr. BURCHETT. I am surprised quite often how often medical records and things, photographs, things like that, are taken out of specifically doctors.

Dr. LEFFLER. Yes.

Mr. BURCHETT. Mr. Rubin?

Mr. RUBIN. Thank you, sir. So, I would break it up into what we can do in the public sector side and then, you know, within private sector organizations. On the public sector side, I think bringing continued awareness to the problem, like we are doing today, is very important. I think continued support for local and state governments, as we discussed, the grant program, programs like that are phenomenal that provide a lot of resources.

On the private sector side, I think it is a lot of the adoption of technology that we heard about here today, getting visibility across your state, both externally and internally, with different tools, leveraging AI and other technology to separate the signal from the noise so you can see and respond to what is important because no

organization can fund the staff and the expertise that they need to do that without the help of technology. And then it is adopting best practices. There is a paradigm called Zero Trust, which is defense in depth and aligned with essentially what you need to know, and last, having a plan to respond.

Mr. BURCHETT. All right. Well, I am about out of time, but I would state to the Committee, as elected officials, something we ought to be very much aware of, if they are reaching into these systems to take something out, they can reach in and put something in. And as elected officials, that is something we need to worry about, and I worry very much about Ms. Mace pointing at her timer and giving me the look.

Ms. MACE. You are over.

Mr. BURCHETT. My time is over. Thank you.

Ms. MACE. Thank you, Mr. Burchett. I would like to now recognize Congresswoman Norton.

Ms. NORTON. Thank you, Madam Chair. Mr. Schneider, every year since 1997, information security and cybersecurity has been on GAO's governmentwide High Risk List, meaning it is extremely vulnerable to waste, fraud, abuse, or mismanagement, or in great need of transformation. This year is no different. In this year's update, however, GAO noted the Biden-Harris Administration's continued commitment to making sure our Nation works to remain ahead of ransom attackers. As always, though, more work can be done, especially as Federal Agencies remain high-value targets for foreign adversaries like Russia and China. Mr. Schneider, why are Federal Agencies such ripe targets for ransomware?

Mr. SCHNEIDER. So, I think Federal Agencies are ripe targets for cyber incidents, in general, because of the information that Federal Agencies have. And so, I think nation-state actors look at Federal, public-sector organizations as having the high-value assets, and, therefore, they are high-value targets as well. And so, they are seeking to get the information from those organizations.

Ms. NORTON. Well, if that is so, Mr. Schneider, what steps can Federal agency leaders take to mitigate their risk of falling victim to ransomware?

Mr. SCHNEIDER. Ma'am, there are certainly defensive steps that they can put in place. You know, my colleague mentions Zero Trust, which is a movement toward, you know, further hardening your infrastructure. I mentioned in my opening testimony implementing multifactor authentication, encrypting your own data, ensuring you have backups. There are, in a lot of ways, some very basic steps that need to be done, patching your systems. They just have to be done very, very consistently and continuously if Federal agencies are not going to get to a point where they are "done" or they are safe. They are going to have to continue to exercise to stay hopefully one step ahead of the malicious actors.

Ms. NORTON. Well, Mr. Schneider, you have previously highlighted to this Committee the need to update Federal information security and cybersecurity laws such as FISMA. So briefly, how could Congress update FISMA or other cybersecurity laws to help agencies better defend against ransom attacks?

Mr. SCHNEIDER. Yes. Thank you for the question. I think an update to FISMA would be timely. It is certainly something that

would help drive the Administration to have some updates. I think codifying the role of the Federal Chief Information Security Officer would be helpful inside of the Office of Management and Budget to really help oversee the implementation of the various standards that the National Institute of Standards and Technology and others put in place. So, there are some governance and oversight that I think an update to FISMA would be helpful for.

Ms. NORTON. Mr. Schneider, earlier this year, in February, the U.S. Marshals Service fell victim to a ransomware attack that reportedly required a months-long recovery. In June, criminal ransomware perpetrators targeted several other Federal agencies, including the Department of Energy. I do not think it takes much imagination to envision the detrimental effects of an attack on the agency responsible for our nuclear resources. So, Mr. Schneider, how can Federal agencies prevent ransomware attacks?

Mr. SCHNEIDER. So, ma'am, I think that is the question of the day of what both Federal agencies and private sector organizations can do to adequately protect themselves, and, again, there are a lot of basic cybersecurity controls that they need to maintain focus on. All organizations need adequate funding to be able to implement those, and they need leadership that is highly focused on the risks and threats that their technology environment brings to them.

Ms. NORTON. Yes. In the case of the June ransomware attacks, I talked about the ransomware criminals were able to exploit a commonly used file transfer program called a MOVEit. So, Mr. Schneider, why might these criminals target contractors and third-party software if their target is the Federal Government?

Mr. SCHNEIDER. Ma'am, if a malicious actor is trying to get toward whatever their target organization, in this instance, a Federal agency, they are going to seek the easiest, quickest, most efficient path to that. And so, they are not just going to look at the Federal systems, they are going to look at all of the systems connected to the Federal systems of where can they get into the information that they are trying to get to.

Ms. NORTON. Thank you. I yield back.

Mr. FALLON. [Presiding.] Thank you. The Chair now recognizes my good friend from North Carolina, Mr. Edwards.

Mr. EDWARDS. Thank you, Mr. Chair. Mr. Schneider, I apologize if this question has been asked before. I just came in from another committee meeting, and it is probably so obvious, someone has to have asked it. Who is behind the majority of the ransomware attacks?

Mr. SCHNEIDER. So, based on the information I am seeing, the majority of the threat actors are housed in or coming out of Russia.

Mr. EDWARDS. Are who coming out?

Mr. SCHNEIDER. Russia.

Mr. EDWARDS. Is there any evidence that these attacks are government-sponsored, or are they just bad actors inside of other countries?

Mr. SCHNEIDER. I think there is mixed on that. I think a significant portion of them, probably the majority of them, are criminals and criminal actors. Now, I think many of those are endorsed by and perhaps even supported by the nation-states within where they reside, to include Russia. I think, in general, my personal opinion

is nation-state actors that are looking for espionage or other foreign policy objectives are less likely to use ransomware as an attack vector.

Mr. EDWARDS. And so, a follow-up to that, I will ask this of the panel, if anyone has any information. Is there any evidence that you are aware of that these bad actors are supported by a government entity of which we should be aware in our interaction with other governments? I mean, it seems like if they are government sponsored, we should hold them accountable or refuse to have different levels of cooperation.

Mr. SCHNEIDER. Well, I think there is certainly evidence of some countries supporting ransomware actors. North Korea is certainly a very good example where they have, you know, as a nation-state, will use ransomware to get around sanctions and try to bring money into the economy.

Mr. EDWARDS. Does anyone else have an opinion or an insight on that question?

Mr. RUBIN. Congressman, I would add that I agree with my colleague.

Mr. EDWARDS. And thank you. So, my understanding of ransomware is, typically, some bad actor is trying to just lock up a computer or encrypt information in return for money. Is there any evidence that these bad actors are trying to capture information, or are they just trying to encrypt someone else's information for extortion?

Mr. SCHNEIDER. I think more and more, we are seeing kind of multi-extortion events where they will both steal the information and try to encrypt it and prevent the owner of the information having access, and then they can ransom them on two fronts, right? The first ransom is "pay me money in order to have access to your systems again," and then a second approach is, you know, maybe the organization has good backups and says I do not need you to restore my services. Then they will threaten the, "we are going to publicly disclose or sell or otherwise compromise the sensitive information." So, we were seeing more and more actors that are also stealing information.

Mr. EDWARDS. And being a part of the private sector and also having served on the board of directors of a bank, I know that one of the things that keeps us awake at night is protecting our data. Have you found that for the private sector, there is any commercial software out there that adequately protects workstations in offices and at homes? And I am not going to ask you for a recommendation. I would just like to know your opinion on how well we are prepared with these third-party packages to protect Americans.

Mr. SCHNEIDER. I would say, I think, in general, the cybersecurity community and cybersecurity tools continue to get better and the malicious actors, you know—it is an arms race, if you will. And so, as we get better on the defensive side, malicious actors are able to leverage new technologies. We talked a little about AI earlier as ways to advance and increase their capabilities, too, so it is a continuous battle.

Mr. EDWARDS. And so, last question for any of you, is our government cooperating in any way or interacting with those third-party

software solutions on what we find to help build better packages for the private sector?

Mr. RUBIN. Congressman, I can speak to that. I work for Palo Alto Networks, and we are a manufacturer of many of these software programs. And we absolutely work regularly with the Federal Government as well as with CISA and other organizations to share the threat intelligence that we see, as well as the capabilities of our software to help protect those organizations.

Mr. EDWARDS. All right.

Ms. MACE. Thank you.

Mr. EDWARDS. Thank you. Madam Chair, I yield.

Ms. MACE. [Presiding.] Thank you. I would now like to recognize Mr. Lynch for his 5 minutes.

Mr. LYNCH. Thank you very much. First of all, I want to thank Chairwoman Mace and Chair Fallon, as well as Ranking Member Connolly and Ranking Member Bush, for convening this joint hearing. I also want to thank the witnesses for your willingness to help the Committee with its work. We have been at this a while, and I am not sure if things are getting any better.

We recently had a sizable ransomware attack, a very high impact in Massachusetts, my home state, on Point32Health, which is the second-largest health insurance provider in Massachusetts. It is the parent company of Harvard Pilgrim Health and Tufts Health Plan, so it affected an awful lot of people. In April of this year, the company announced that it had been targeted by a ransomware attack that forced a shutdown of several critical systems used to service members' accounts, brokers, and also healthcare providers. The attack also involved the theft of very sensitive information.

So, as Mr. Schneider was saying, this was one of those cases where they could have a denial of service, or they could just simply sell the sensitive information. So, it compromised the personal information of more than 2.5 million current and former subscribers, dependents, or providers, and, unfortunately, the stolen data included Social Security numbers, medical history data, health insurance account information, and taxpayer ID numbers, so a very, very tough situation.

Importantly, the American Hospital Association has since warned that the frequency, sophistication, and severity of ransomware attacks against our healthcare sector is dramatically escalating with organized criminal gangs and military units replacing rogue individual actors as the primary perpetrators. As a matter of fact, in the first 6 months of 2023 alone, more than 220 cyberattacks targeted hospitals and healthcare systems with over 36 million people affected.

So, Dr. Leffler, speaking directly, look, healthcare is different. In some ways, there is a vulnerability there that is not present in some others. The impact goes beyond just the institution. It is all those people whose, you know, private health information that is out there. From your experience, and, you know, from the way you have looked at this, are there certain steps that healthcare institutions need to be taking right now and that you have taken perhaps through your experience in Vermont that might make the system more secure?

Dr. LEFFLER. Thank you for the question. First, have a strong separate protected backup. Critically important, have it separated from your normal system and updated every single day. Next, make sure your IT team is empowered to shut down the system immediately if necessary. Do not make them go up the chain of command. If they see something unusual, shut it down immediately. Most importantly, from clinical care to this point before the cyberattack, we typically did a drill where we would have our EMR down for 2 days, which seemed like a really long time. We were down for 28 days. The things you do over 28 days are vastly different. So, I would recommend all hospitals or healthcare systems at least to a tabletop exercise to imagine what it would be like to be down for a month. You did not have phones, schedules, no way to get lab results to the floors. How would you handle that I think is critically important. Thank you.

Mr. LYNCH. Yes. The wider impact is now, in the Massachusetts case, we are seeing class action lawsuits against the institutions because of the poor handling of the information, so there is a follow-on problem there. Given the fact that, you know, we are all in the patient gateway system—that is what mine is called with my hospital, so all my medical records—so, we are moving to, you know, mobile applications for all this information. Is there some way that we might close that gap?

I mean, there was an article in the Journal of Medicine, like, a month ago, 2 months ago, that said we should treat these as sort of regional disasters almost because of the community-wide impact that it is having, not just on the healthcare institution, but on the community in general. I would just like to get your thoughts on that and about those longer-term impacts on the credibility of the either insurance company or the hospital, and then, you know, how you clean that up, even though the trend is moving to, you know, greater mobility and easier access to this digital information.

Dr. LEFFLER. In Vermont, this was a disaster.

Mr. LYNCH. Yes.

Dr. LEFFLER. It impacted our entire state, impacted all 14 hospitals. It affected patients across our region. It was clearly a disaster, and we are grateful that our Governor and National Guard stepped in to help us. In terms of better protection, I really think the best, and once again, I am at the edge of my knowledge here, but the best we can do is break the system up into lots of little pieces, so if someone gets in somewhere, they have a very hard time getting in everywhere. And we have added a lot of steps of multi-identification to protect the system, and we have done a huge amount of education since the attack to make it harder for people to penetrate.

Mr. LYNCH. Thank you. Madam Chair, I appreciate your courtesy. Thank you. I yield back.

Ms. MACE. All right. I would now like to recognize Mr. Langworthy for 5 minutes.

Mr. LANGWORTHY. Thank you very much, Madam Chair, and to both of our Chairs and Ranking Members for putting this together, and to our witnesses. You know, for the longest time, the United States has enjoyed a reputation of being impervious to foreign threats on our soil. But cyber-attacks serve as a prime example of

this contemporary form of warfare and espionage that we all have to be ready for and vigilant against. Even our wealthiest corporations or financial institutions or hospitals or our civic organizations with cutting-edge cybersecurity protocols, they can fall prey to these cyberthreats. As we witness breaches in our major urban centers, we must consider the potential harm that can be inflicted on our rural communities, such as those in my district, in New York's 23d congressional District. We are home to many rural hospitals, school districts, educational institutions, and they are very vulnerable to these challenges.

With that being said, Dr. Leffler, you highlighted in your testimony that UVM Medical Center has unfortunately experienced several cyberattacks in the past. Can you identify any recurring patterns among the perpetrators? Were these incidents typically orchestrated by cybercriminals seeking financial gain, or are these foreign actors primarily interested in obtaining sensitive patient information?

Dr. LEFFLER. Thank you. Gratefully, we only suffered one cyberattack. It was in October 2020. It did affect every part of our system. We did not contact the cybercriminals or pay ransom, but I am sure they wanted both payment to reopen our system and likely would have sold the information if they got it. We are fortunate that they were unable to get into our system to gain patient information. So, we suffered one attack. At the time, it was during the pandemic. We had many people working from home, and we did that very quickly. And so, we have added a lot of security around our computer systems, laptops, and that was the way they got in. Someone had gone home with their laptop and it entered from a home user when they plugged it back into our system. That is how it got into our network.

Mr. LANGWORTHY. Thank you. We are all familiar with the financial ramifications of ransomware attacks from cybercriminals. The losses could be in tens of millions of dollars or more. For a major hospital that is perhaps manageable, even if it is not ideal, but let us talk about situations where perpetrators are seeking data and not dollar value. Dr. Leffler, when actors target our constituents' medical records and data, what specific purposes do they have in mind for acquiring this information, and what threat is the data leak to patients?

Dr. LEFFLER. It is a very significant threat to patients. Patient information is protected by HIPAA. We take that very seriously. And if a cybercriminal is able to get into the electronic medical record, they can sell that information on the internet and access both patient's financial information, insurance information, and cause huge issues for our patients.

Mr. LANGWORTHY. Thank you. There is no doubt that hospitals are hurt in these situations. I mean, their reputation and their community all get negative public spotlight, but the primary focus for any hospital is undoubtedly patient care. I understand that ransomware attacks can result in unauthorized access to sensitive information, but could you elaborate on how such attacks might potentially affect the quality of patient care?

Dr. LEFFLER. Basically, in healthcare right now, your electronic medical record is your connection to everything that you do. Every-

thing runs through that. All of your lab information, radiology information, patient care, transfers, all run through that. When that system goes down, it has a huge impact on patient care. Right now, if you are going to order a medication for a patient, electronic medical record tells you if you have picked the correct dose, the medication is right for the intended purpose, if there is an allergy, if it is safe to give this particular patient based on their size and age. When that system goes down, all those things revert back to a system that many of our doctors now are no longer trained on.

And so, we had to go back to paper and make sure that someone, a person, was going through and doing all those steps every time we ordered anything. It impacts how you run your operating room, how lab results are stored, how imaging is done. We had to buy a bunch of drives to store imaging while we were down. It has a huge impact on patient care every day, and for the University of Vermont Medical Center, the impact was greater than the pandemic.

Mr. LANGWORTHY. It seems like that would have tremendous impact on your workforce as well. What resources has the Federal Government offered to hospitals that have experienced ransomware attacks, and are there any specific recommendations or standards that you would propose to this Committee, particularly in the context of rural hospitals?

Dr. LEFFLER. The FBI was hugely helpful during our cyberattack and provided great insight and help. Beyond that, I said before hospital budgets are very tough, and typically, hospital leaders want to spend money on patient care issues. So, grants or funding to help have the most current cybersecurity protection would be very useful. Guidance and training around how to prepare for a 30-day outage, I think, is critically important in helping to make sure that they have the most current EMRs, people, training will make a difference.

Mr. LANGWORTHY. Thank you very much. Thank you for your testimony, and I yield back.

Ms. MACE. Thank you. I will now recognize Congressman Fry for 5 minutes.

Mr. FRY. Thank you, Madam Chair, and thank you to Chair Fallon and the Ranking Members for having this hearing today. Thank you for being here. You know, ransomware attacks—of course we have talked about this today—are becoming increasingly frequent in our society, particularly as we rely more and more on technology. My home state of South Carolina is not immune from that. We were subject to a very serious and costly attack in October 2012 when the South Carolina Department of Revenue was hacked by cybercriminals who used encrypted malware to steal the income tax returns of 6.4 million South Carolinian residents and businesses. The attacks impacted more than three-quarters of our population, 3.6 million Social Security numbers, 387,000 credit and debit card numbers. The financial cost, when I was a member of the General Assembly, was over $20 million to protect South Carolinians. At the time, this was considered to be the biggest and largest attack on a state agency, not only in South Carolina, but across the country.

Just this year, South Carolinians have been subject to numerous attacks, and it does not seem to have an end in sight. We have all witnessed agencies, hospitals, businesses, people individually, who have run into this problem. And so, the question that I have, for you, Mr. Schneider, is, of the cybercriminals that you have encountered in your 30 years of experience, who are these people? Are they young, are they old, are they lone wolves, are they domestic, are they foreign actors? What type of people do you see, that engage in this practice?

Mr. SCHNEIDER. Thank you for the question, Congressman. I think it has evolved over time. I mean, sort of the stereotypical from 30 years ago was, you know, a kid in their garage on a big couch. And, I think what it has really moved on to is, you know, what we are seeing today are, you know, ransomware actors, cybercriminals, they are thinking like business people. They are setting up help desks so that if a victim does not know how to, you know, pay them appropriately, they can help them, you know, set up an appropriate wallet and be able to send them money.

So, Chairwoman Mace mentioned earlier ransomware as a service. So, this is becoming a business enterprise for the malicious actors that are very, very organized. They are typically, at least, in nation-states that are allowing them to, you know, to act pretty freely, and sometimes they are probably encouraging them as well.

Mr. FRY. You know, we hear all the time that cybercriminals adapt their tactics to infiltrate. How do, in your eyes, these cybercriminals become involved in this activity? How do they get engaged in their craft?

Mr. SCHNEIDER. Congressman, I do not have much data or information on kind of how they get into this. Part of my speculation is that, you know, they are probably in countries where, you know, if they have some skills, this is a place where they can put their skills, you know, to unfortunately work in a malicious manner. We would much rather see them on a defensive side of the cyber equation someplace.

Mr. FRY. Has the approach of cybercriminals changed at all in kind of this era of work from home, you know, during the pandemic? How has the landscape shifted?

Mr. SCHNEIDER. I think the landscape has shifted in the way that our threat surface is connected, and, you know, we have discussed earlier, we continue to interconnect more and more systems, more and more data. And every time we interconnect more systems, we introduce potentially additional vulnerabilities that give the actors, you know, more places to attack from.

Mr. FRY. Thank you for that. Mr. Rubin, in your testimony, you cite that a recent Unit 42 report found that our security teams take nearly 6 days to resolve an alert. According to the report, the amount of time it takes adversaries to move from compromise to data exfiltration is merely a few hours. Do you expect 6 days to remain the average in the future, given that cybercriminals are becoming increasingly sophisticated and effective?

Mr. RUBIN. Thank you, Congressman. So, our goal is to help organizations reduce that time to respond. So, combination of training, combination of technology, combination of dedicated resources, our goal is to help organizations move that from 6 days down to

hours or even minutes. When a threat actor gets into an organization, they might have a foothold on one system, and what they are trying to do is to elevate privileges to break out of that system and to move into other parts of the network. So, if you can catch them when they are on that first system, and you can contain it and take what might otherwise be a crippling ransomware attack and make that something much smaller.

Mr. FRY. Thank you for that. Within that 6-day period, how disruptive is that to businesses and employees?

Mr. RUBIN. Of course, Congressman, it absolutely varies on a case-by-case basis. But what I can tell you a recent incident response investigation that we did, we saw for a major tech company, within a matter of 15 hours, the threat actor went from a phishing attack to escalating privileges to moving laterally to exfiltrating over a terabyte of information and locking up 10,000 systems. Fifteen hours.

Mr. FRY. Fifteen hours.

Ms. MACE. All right. Thank you, Mr. Fry.

Mr. FRY. Thank you.

Ms. MACE. All right. In closing, I want to thank our panelists this afternoon, once again, for their testimony today, especially for those who talked about the ransomware attack they had. Very few organizations, institutions, and agencies will actually speak publicly about these experiences out of fear. And I appreciate the collaboration between my colleagues on this and for everyone having the courage to be here today.

I would now like to yield to Ms. Norton for closing remarks.

Ms. NORTON. Thank you, Madam Chair. First, I want to share the concern my colleagues expressed earlier about these attacks on critical infrastructure. That is why we conducted a comprehensive investigation which provided new insights into how ransomware attacks unfold. I would like to submit to the record some of the findings we released in a memo to Congress. Would you give this to the staff?

Ms. NORTON. Finally, I want to thank my colleagues for calling this important hearing on ransomware today, but I want to highlight the paradox of their efforts to combat ransomware and cyberattacks. At the same time, they are driving us headfirst into a government shutdown. A shutdown will have real-world effects both in cyberspace and our communities. As both Mr. Connolly and Ms. Brown indicated in their opening statements, the Cybersecurity and Infrastructure Security Agency, the Agency that leads Federal cybersecurity efforts and serves as a national coordinator for critical infrastructure security and resilience, will furlough thousands of its employees, 80 percent of its workforce, in fact. The Department of Justice, the Agency responsible for investigating and taking down criminal ransomware attacks, will also be forced to furlough thousands of employees. Those are just two agencies.

A shutdown hurts our communities nationwide and at their core. While we think all Federal employees are in the Nation's Capital here, the congressional Research Service has found that every single congressional district is home to at least 2,600 civilian Federal employees, all of whom do not know when they will receive their next paycheck. Our military service members will continue working

every day to keep our country safe, including our 1.3 million active service troops, but they will not receive a paycheck until the government reopens. That figure includes 11,000 service members in my district, 114,000 service members in Texas, and 38 service members in South Carolina. Many of these military families will struggle to pay rent, afford groceries, or get their prescription medications. I suppose that is one way to thank those who put their lives on the line for their Nation.

Democrats are not the only ones horrified by the MAGA Republicans holding our Nation hostage. Take, for example, my colleague, Mr. Bacon, who told reporters that the Republicans are currently "the dysfunction caucus at work." My colleague, Mr. Graves from Louisiana, said the Republican holdouts on appropriation government were "holding disaster victims hostage." And Mr. Garcia said of the MAGA extremists that "they just handed a win to the Chinese Communist Party." If my colleagues really cared about national security, cybersecurity, and the health of this Nation, they would be funding the Federal Government right now. Like the ransomware attackers we examine throughout this hearing, our Republican colleagues are holding the Nation captive, and I yield back.

Ms. MACE. Thank you. I now yield to Chairman Fallon for closing remarks.

Mr. FALLON. Thank you, Madam Chair. Just a couple of things. One, it is amazing that you think something like combating ransomware would not be partisan, and some of our colleagues did not make it partisan, some did, calling folks MAGA extremist and people that want to shut down. I do not know anybody that wants a shutdown. And when you talk about resources, there are limited resources, and that is why a CR that we are trying to work out to attach some border security that we desperately need, and maybe a modest cut of 8 percent of discretionary spending when we are spending $663 billion on debt service just this year alone. And according to CBO, over the next decade, it is going to be $11 trillion additional dollars to service the debt, that in a decade from now, the interest payments on the debt could equal, if everything stays the same, about half of our total of discretionary spending. It is time to do something.

And so, it is sad to see that, but you want to talk truths and facts. The Senate, which is controlled by the Democrats, had passed all their appropriations bills out of committee before the August recess and sat on their hands, Chuck Schumer did, for 2 months, and did nothing. So, you want to call it something, you can call the Schumer shutdown. Let us hope it does not even happen. I am not rooting for it, but it does seem some people are, and that is sad, playing politics on something like this.

Now, on ransomware, we want to deal with specificity. I have a friend of mine I had mentioned earlier, anonymous friend, he has texted me now and he says do not forget to tell them to have really good backups, have multifactor authentication, and need help from the government to get after these guys as well. And one of the things we can do to get after them is I filed the bill last Congress, H.R. 3388, which is Protecting Critical Infrastructure Act, which would expand penalties for fraud and related activities on these

kind of attacks on our critical infrastructure—Colonial Pipeline, JBS, would be something along those lines that would fit into that—and expand the penalties.

Now, I know it is hard to get our hands on these folks, considering most of them are in countries that would protect them or at least look the other way. Russia and China come to mind, but sometimes they get careless, and we need to also make sure and clearly define in statute that it does not need to be physical infrastructure to be critical. It could be cyberspace infrastructure. The laws were written 30 years ago when there was not even a cyberspace, or 40 years ago. And then also, my bill would direct the President to impose sanctions on foreign persons who attempt to harm United States' national security interests by accessing and compromising our critical infrastructure. So, there are those things as well that we can do. So, I am glad that we have had the opportunity to have partially a bipartisan meeting on these issues.

Mr. Schneider, you mentioned the battle between hackers and the organizations these bad actors are targeting is becoming, you know, an arms race and a term that I think we should really think about and give a lot of weight to. And while I think that is accurate, it also denotes the threat posed upon America by Russia. And we have heard that these attacks are originally mostly there and something that we need to protect small, medium, and large interests.

So, I hope that in the future, we can have maybe someday, maybe I am just naive, but have a hearing that is something that has nothing to do with partisanship, that we can look and focus directly on the specificity of the threats, and come up with some solutions because, believe it or not, ladies and gentlemen, we have some smart people in Congress. We got some dumb people, too, but we got some smart ones, and maybe we can work together because having served for 8 years in the Texas legislature, not everything was partisan there, and I think we need to bring a little more Texas to Washington, DC. Madam Chair, I yield back.

Ms. MACE. Thank you, and I will now recognize myself for a few minutes. In closing, I did want to say that because, you know, the White House did such a good job about sending their talking points to this hearing this afternoon, that in the event that there is a shutdown, that 80 percent figure the White House is pushing of CISA employees who will not be showing up to work, that is a decision by the President of the United States and his Administration to decide what percentage of CISA employees are deemed essential and not will be showing up to work in the event that there is a shutdown. In the event that there is a shutdown, it is up to the President of the United States and his Administration to prioritize who is and who is not essential. They can make it as painful as they want or as painless as they want in this thing. And by law, any Federal employees who are furloughed are going to get back pay, so, you know, that is something that should be very clear.

If we could just tell the God's honest truth in this thing, we would not be pointing fingers at either side because, guess what? Both sides are to blame if there is a government shutdown. Just this week, we saw $33 trillion added to our Nation's debt, and that sham of a debt ceiling deal that the American people were sold a

bed of lies on is going to add $18.8 trillion to the debt over the next 10 years. We are talking about $50 trillion in debt over the next decade, and they just want to blame each other. No, both Republicans and both Democrats are at fault.

The last time we balanced a damn budget in this place was in the 90's under President Clinton, a Democrat President and a Republican-controlled House. They had a decade plan to balance the budget. They did it in 4 years because of surplus tax revenue. We cannot even get a plan to balance the budget up here in the next 20 years. So, when the American people get pissed off about a government shutdown, blame Republicans and blame Democrats who are at fault and refuse to get to the table to make the spending cuts that are necessary to get this country turned around in the right direction.

So, with that, and without objection, I am going to ask unanimous consent to enter a letter from the Electric Reliability Council of Texas or ERCOT into the record.

Without objection, it is so ordered.

Ms. MACE. Now we are back to ransomware—to go off on spending—and without objection, all Members will have 5 legislative days within which to submit materials and to submit additional written questions for the witnesses which will be forwarded to the witnesses for their response.

Ms. MACE. And if there is no further business, without objection, the Subcommittee stands adjourned.

[Whereupon, at 2:46 p.m., the Subcommittee was adjourned.]

○