HOUSE ENERGY AND COMMERCE SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS

"Stopping Digital Thieves: The Growing Threat of Ransomware"

July 20, 2021 – 10:30 AM

OVERVIEW

On Tuesday, July 20, the House Energy and Commerce Subcommittee on Oversight and Investigations held a hearing entitled, "Stopping Digital Thieves: The Growing Threat of Ransomware." During the hearing, Members and witnesses discussed: cyber hygiene; operational technology security; healthcare cybersecurity; public-private partnerships; cryptocurrency and ransom payments; and foreign adversaries.

OPENING STATEMENTS

- Subcommittee Chairwoman Diana DeGette (D-CO)
- Subcommittee Ranking Member Morgan Griffith (R-VA)
- Committee Chairman Frank Pallone (D-NJ)
- Committee Ranking Member Cathy McMorris Rodgers (R-WA)

WITNESS PANEL

- Ms. Kemba Walden – Assistant General Counsel, Microsoft Corporation
- Mr. Robert M. Lee – Chief Executive Officer and Co-Founder, Dragos
- Dr. Christian Dameff, M.D. – Medical Director of Cybersecurity, UC San Diego Health
- Mr. Charles Carmakal – Senior Vice President and Chief Technical Officer, FireEye-Mandiant
- Mr. Philip Reiner – Chief Executive Officer, Institute for Security and Technology; Executive Director, Ransomware Task Force

QUESTION AND ANSWER SUMMARY

Cyber Hygiene

Chairwoman DeGette noted senior cyber experts from the government have expressed concern about some of the private sector's compliance with cyber hygiene requirements and the limits of the federal

government's existing authorities to manage the problem. She asked the panel for the most impactful actions Congress should take. Mr. Reiner suggested requiring organizations to meet baseline cybersecurity requirements in order to receive national grants. Mr. Carmakal agreed tying government grants to security standards generally sounds like a good idea. Chairwoman DeGette highlighted Ms. Walden's testimony, which cited an estimation that more than 99 percent of cyberattacks would have been prevented if multi-factor authentication was deployed. Chairwoman DeGette inquired if basic cyber hygiene requirements should be mandated through legislation. Ms. Walden agreed basic cyber hygiene principles should be required. Mr. Lee suggested more resulted-oriented policy since prescriptive requirements may not be applicable across different infrastructures. Mr. Carmakal recommended organizations learn from other breached entities and adopt recommendations from incident response exercises, such as those in Mandiant's white paper.

Rep. Ann McLane Kuster (D-NH) cited Ms. Walden's testimony that applying basic cybersecurity hygiene can prevent a cybercriminal's ability to ransom a system. Ms. Walden explained enabling multi-factor authentication, training employees and staff to identify phishing, and segmenting the network are some of the simple cyber hygiene activities that small and medium businesses can and should take to prevent cyberattacks. Mr. Carmakal added companies should provide technology to block malicious emails and install security patches across the environment. Rep. Kuster inquired if "investments in cybersecurity are good returns on investment." Mr. Reiner replied affirmatively, arguing investing upfront is more affordable than having to reconstitute the entire organization after an attack.

Rep. Jan Schakowsky (D-IL) noted cybercriminals are getting more sophisticated and "we are playing catch up." Mr. Carmakal explained it is exhausting for incident responders to constantly deal with highly disruptive attacks against organizations. Rep. Schakowsky asked if there should be requirements for building in these security systems. Mr. Carmakal replied there is a general expectation for most organizations to have cyber security controls and resiliency in place. Rep. Schakowsky questioned where the responsibility lies and if the government should step in if there has been a failure in security. Mr. Carmakal argued there should be a shared responsibility between victim organizations, security companies, and government because this requires a concerted effort. He highlighted the success of the FBI notifying victim organizations about upcoming intrusions.

Operational Technology Security

Rep. Jerry McNerney (D-CA) remarked operation technology (OT) system attacks are increasing in severity and frequency. He noted Colonial Pipeline proactively shut down its OT systems in response to ransomware attacks on its IT system. Rep. McNerney asked Mr. Lee how serious and widespread the ransomware threat is on OT systems. Mr. Lee replied, "it is significantly more frequent than people would realize." Rep. McNerney asked if there is any government support for companies dealing with live OT threats. Mr. Lee explained OT cybersecurity expertise is more in the private sector than in government. He emphasized the need to remove barriers to get visibility in those systems. Rep. McNerney asked Mr. Carmakal about the risks posed by ransomware attacks on OT systems and how potential victim organizations can best protect themselves. Mr. Carmakal replied, "ransomware attacks against operational technology systems have the potential to be incredibly devastating." He noted many organizations generally "struggle to think about security from an operational technology perspective."

Healthcare Cybersecurity

Chairwoman DeGette inquired about specific issues in the healthcare industry and what the Committee should do to ensure good cyber compliance. Dr. Dameff emphasized the need for additional information because it is "very difficult to measure the impacts of a cyberattack on a patient."

Ranking Member Griffith asked Dr. Dameff if multi-factor authentication works in time-sensitive settings like emergency rooms. Dr. Dameff explained many hospitals are deploying multi-factor authentication to protect patient data; however, he agreed patient care cannot be hindered in the emergency setting by overly burdensome security controls. He emphasized the importance of preparing for an inevitable attack by

maintaining a backup system to help restore patient care quickly. Ranking Member Griffith inquired how expensive it will be to establish good cyber hygiene, noting many competing hospitals have merged due to financial stress. Dr. Dameff agreed the consolidation of healthcare has increased the risk to patient safety from ransomware attacks because of the shared infrastructure and technology among many hospitals. Dr. Dameff noted many hospitals already have manual non-technical processes to take care of patients during emergencies, and he argued they should enact those plans to prepare in a cyber context as well. Dr. Dameff acknowledged it will be costly to implement many of the technical controls and many hospitals are already resource-stricken, particularly due to the COVID-19 pandemic. Ranking Member Griffith inquired if there should be some liability protection for hospitals meeting a minimum requirement. Dr. Dameff voiced support for incentivizing instead of penalizing hospitals for trying to take care of patients. He suggested tying reimbursements to meeting a certain cybersecurity threshold.

Rep. Michael Burgess (R-TX) questioned if reputational damage is a disincentive to reporting a cyber incident. Dr. Dameff agreed individual organizations may delay reporting until they are able to anticipate what might be a large punitive fine and they are also occupied with trying to restore operational capacity. Rep. Burgess asked if there should be something like the Strategic National Stockpile to keep hospitals functioning during a ransomware attack. Dr. Dameff acknowledged hospitals would benefit from deploying a resource like FEMA's Disaster Medical Assistance Teams (DMAT) to help alleviate patient care constraints while restoring systems. Rep. Burgess questioned if hospitals know the downstream impacts on patients following an attack. Dr. Dameff replied negatively, and he urged mandatory reporting for severe attacks on patient safety implications. He noted one of the barriers to reporting is that the systems for measuring care quality and patient safety are themselves targets of the ransomware. Dr. Dameff voiced support for additional metrics on ransomware attacks.

Ranking Member McMorris Rodgers argued “when the hospitals are hit, it can literally be life or death.” She asked Dr. Dameff to explain the cyber threats hospitals face and how they can impact patient health. Dr. Dameff noted clinicians are very dependent on technology for treatment and diagnosis, so they would be unable to do their jobs if a large ransomware attack takes down these technical systems. He added without technology, it takes longer to get test results to make decisions on things like antibiotics for severe infections, or to identify when patients have certain conditions. Dr. Dameff emphasized these types of attacks are exceptionally chaotic with a lot happening at once, so the ability for hospitals to report on patient impact is nearly impossible as they attempt to restore their systems. Ranking Member McMorris Rodgers asked how hospitals can better secure their networks against cyberattacks. Dr. Dameff recommended hospitals prepare for an inevitable ransomware attack and practice taking care of patients without technical systems.

Rep. Neal Dunn (R-FL) highlighted the significant uptick in ransomware attacks on healthcare organizations since 2016. He asked Dr. Dameff about the biggest vulnerability in healthcare. Dr. Dameff argued the hyperconnectivity of healthcare accelerated over the last decade was not paired with the commensurate security required. He noted healthcare is “generally a soft target for cyberattacks and ransomware” and the pandemic has further constrained many health organizations.

Rep. Raul Ruiz (D-CA) inquired about the kind of procedures hospitals need to be able to effectively operate during a ransomware attack. Dr. Dameff expressed support for the preparation of hospitals to operate in a manual fashion while the systems are being restored after a ransomware attack. He noted hospitals already have mandatory processes in place to prepare for other hazards like earthquakes and hurricanes.

Rep. John Joyce (R-PA) asserted Congress must take a proactive approach to strengthen critical infrastructure and ensure Americans’ medical data is safe. Rep. Joyce asked how long the systems are down after a hospital or healthcare system is the victim of a ransomware attacked. Dr. Dameff explained cyberattacks are increasing in sophistication and frequency, so he sees more of a trend towards weeks to months of downtime following these “devastating” attacks. Rep. Joyce questioned if the healthcare system

reverts to manual patient care systems during the recovery response. Dr. Dameff replied, “physicians should be trained to operate in conditions that do not have technology, or to rely on less connected technological backups as a stopgap measure for patient care.” Rep. Joyce asked if backing up the system in the cloud is a “foolproof” way to prevent or mitigate the effects of a cyberattack on healthcare systems. Dr. Dameff argued they will not see the trend towards centralization of medical device management or electronic health records into the cloud. He explained the centralization into the cloud means that a single attack on a cloud provider offering services to many hospitals could impact all of them at once.

Rep. Scott Peters (D-CA) inquired if hospitals should be more disconnected or fenced off to operate and connect internally without being so exposed. Dr. Dameff voiced support for investing in technology that limits the exposure of hospitals since they are often “soft targets” with flat networks. He noted this concept of isolating critical sections of the hospital would require costly technological solutions, so many health care systems will not be able to deploy such technology without additional resources and guidance.

Rep. Kim Schrier (D-WA) asked how sister hospitals, local entities, private sector actors, or the federal government could better support lesser-resourced or rural hospitals. Dr. Dameff emphasized the importance of preparatory efforts to prevent and then mitigate the impacts of attacks. He noted in the response phase, it is common for a hospital to reach out to law enforcement such as the FBI, but interagency communication is lacking and other government agencies like CISA or the FDA are not always involved. Rep. Schrier asked how to inform the public that even with the best preparation, these attacks are so common that a hospital could still be hit. Dr. Dameff argued there should be no competitive advantage in healthcare cybersecurity because no health organization is immune regardless of their cybersecurity budget. He emphasized the need to assure consumers that hospitals are preparing for and mitigating incidents, but these attacks are an unfortunate consequence of the hyperconnectivity of healthcare.

Public-Private Partnerships

Chairman Pallone questioned if they should be doing more to assist U.S. companies, particularly small- to medium-sized businesses, to deal with cybersecurity threats. Chairman Pallone requested Mr. Carmakal to explain the types of resources that companies need once they are hit by a ransomware attack. Mr. Carmakal replied some smaller organizations do not even have dedicated security teams. He asserted the government needs to focus on disruption of ransomware so that smaller organizations without the resources and the staff have some additional government support. Mr. Reiner added CISA, and other departments and agencies, are very well positioned to help share information and provide tools to organizations for free. He emphasized the need to increase awareness around these available tools and services.

Ranking Member McMorris Rodgers and Rep. Tom O’Halleran (D-AZ) inquired how the private sector can partner with the government to address ransomware attacks. Ms. Walden noted the government has legal authorities that the private sector does not have, such as law enforcement authorities and intelligence authorities. She argued the private sector can work with law enforcement to identify criminals and tear down their infrastructure. Ms. Walden emphasized the need for actionable information sharing so the private sector can exchange ideas, signals, and technology with government partners. Mr. Carmakal suggested facilitating a way for victim organizations to share information about active attacks and compromises with some central governing body or agency which will disseminate that information. He highlighted the trend of victims becoming a second victim because of public shaming by other organizations and the public after a cybersecurity incident.

Rep. David McKinley (R-WV) expressed frustration over the lack of progress on addressing cybercrime, and he asserted cyber criminals are exploiting outdated laws. He argued attacks on critical infrastructure could be mitigated with updated reforms or international treaties, including some stiff enforceable penalties. Rep. McKinley suggested developing redundancy in the energy system to restore systems in the event of a hack. Dr. Dameff voiced support for any efforts to increase healthcare resiliency in the face of cyberattacks.

Rep. Paul Tonko (D-NY) argued the government has an important role in ensuring the nation's cybersecurity, especially related to critical infrastructure. He asked Mr. Lee how a critical infrastructure company can seek assistance from the federal government following an attack. Mr. Lee replied there is a lot of confusion on who to call in the government following an attack. Mr. Lee suggested the Cybersecurity and Infrastructure Security Agency (CISA) is well established as a civilian agency to be the coordinator of the interagency process. Rep. Tonko expressed concern one agency cannot understand all the complications of a ransomware attack across industries, which is why there are sector-specific agencies. Rep. Tonko asked how to improve the coordination between DHS, sector-specific agencies, and the private sector to address ransomware threats. Mr. Reiner argued the White House should take the lead in coordinating interagency assets.

Rep. McNerney inquired about the role public-private partnerships could play in shoring up some of these vulnerabilities in OT systems. Mr. Lee explained partnership with the sector can help to government partners understand what the sectors need for OT systems. He noted some cyber best practices such as patching and phishing training are appropriate for enterprise security but are not suitable for operational technology security.

Cryptocurrency and Ransom Payments

Chairman Pallone asked Ms. Walden how small businesses navigate paying a ransom in cryptocurrency. Ms. Walden recommended businesses should not pay the ransom. She noted criminal actors provide instructions to the victim on how to obtain cryptocurrency.

Rep. Kathleen Rice (D-NY) requested Mr. Carmakal expand on ransom payments and the motivation to pay them or not. Mr. Carmakal explained most organizations do not want to pay an extortion demand, but they feel they have no other option to recover business operations or minimize the impact. He recognized there are certain situations in which a company may choose to pay and get some temporary benefit, such as access to their systems and data through the decryption tools provided by the threat actors. Mr. Carmakal noted there are no guarantees that the stolen data will not be published down the road, even if the ransom was paid. Rep. Rice asked Mr. Reiner about the need to understand and regulate cryptocurrency. Mr. Reiner argued cryptocurrency is a major facilitating element of what has accelerated the ransomware threat today. He urged more information exchange and transparency in the government and private sector to better understand the “incredibly complex web” of cryptocurrency.

Rep. Schakowsky inquired about alternatives to paying a ransom. Ms. Walden replied raising the maturity level of potential victims through baseline cyber hygiene requirements can help prevent a ransomware attack in the first place. Ms. Walden recommended a cost recovery fund to help absorb the cost and impact of attacks on critical infrastructure. Ms. Walden also emphasized the need to clarify which department or agency has authority over the crypto economy.

Rep. Palmer inquired if cyber insurance is hurting payment negotiations since criminals may have hacked the insurance companies and know what the victim can pay. Ms. Walden noted she is not a cyber insurance expert, but she explained cyber insurance companies are just one part of the ecosystem supporting victims of ransomware attacks.

Rep. Ruiz noted ransomware cyberattacks are becoming a growing and frequent threat to businesses, utilities, and government agencies. Rep. Ruiz asked about the most significant barriers for companies when faced with a ransomware attack. Mr. Carmakal explained there is a lot of confusion in the early days of an incident and the main goal is to get things back online and assess the true impact of the incident. He noted victims typically call a legal team, incident response organization, and cybersecurity insurance provider. Mr. Carmakal added the complex situation often takes several days or weeks to investigate and recover the environment. Rep. Ruiz requested Mr. Reiner to explain the Ransomware Task Force’s recommendations on ransom payments. Mr. Reiner responded the task force recommends a set of steps to shore up cyber defenses before mandating the prohibition of ransom payment.

Rep. Lori Trahan (D-MA) voiced concern cyberattacks are becoming especially commonplace within critical public service sectors ranging from health care to education. She noted ransomware has become one of the most attractive tools for criminals because it can be very lucrative. Rep. Trahan argued they need to "find ways to disrupt the ability of criminals to demand and receive ransom payments without consequence." She asked Ms. Walden why cryptocurrencies are the chosen method of payment for ransoms. Ms. Walden explained blockchain technology underlying cryptocurrency allows for a decentralized and distributed payment system that can anonymize the person behind the transaction. She added the transactional costs in the crypto economy are much lower than in traditional central banking systems, and cryptocurrency can move quickly and effectively across borders. Rep. Trahan asked Mr. Reiner for his recommendations on expanding the applicability or enforcement of regulations on cryptocurrency. Mr. Reiner responded elements of the cryptocurrency ecosystem could be pulled into existing regulatory regimes, such as expanding the application of know your customer rules or anti-money laundering rules. He noted some of this is outside the United States' jurisdiction, so it is important to work closely with international partners.

Foreign Adversaries

Rep. Dunn expressed concern Microsoft's work in China makes their products more vulnerable to influence by the Chinese government. Ms. Walden emphasized they operate on a zero-trust basis, and they do not store any U.S. data in China. She also noted Microsoft's cybercrimes unit goes after cybercriminals and their infrastructure in "unfriendly jurisdictions" like China or Russia.

Rep. Gary Palmer (R-AL) mentioned the June 14th NATO meeting and their statement addressing the increasingly complex security environment. He stated cyber and ransomware attacks are treated as criminal activity when they are not sanctioned by nation-states, but in some cases the attacks are at least approved by nation-states like Russia and China. Rep. Palmer asked if the military should be used to address this issue. Mr. Lee asserted the military should be the last resort and there are still plenty of mechanisms left to address cyber threats. Mr. Lee also urged the U.S. to draw red lines on what cyber behavior is not tolerated.

--

Please click here for the archived hearing.