Questions for Mr. Amit Yoran
Chairman and Chief Executive Officer, Tenable

Questions from Chairwoman Carolyn B. Maloney

July 15, 2020, Hearing: "U.S. Cybersecurity Preparedness and H.R. 7331, the National Cyber Director Act."

---

1. On March 16, a cyberattack reportedly targeted the computer systems of the Department of Health and Human Services in an unsuccessful attempt to disrupt the Department's response to the pandemic. By the end of March, every country in the world had seen at least one attack in connection to the coronavirus pandemic. Do you think America's role in the international coordination and response to these threats would have benefitted from a National Cyber Director?

Yes, I think America's role in the international coordination and response to targeted attacks related to the pandemic would have benefitted from a National Cyber Director. Over the past several months, cybercriminals have leveraged the current COVID crisis by increasing malware and phishing campaigns. Cyber criminals are advantageous actors and will continue to target known weaknesses during times of upheaval and crisis.

As cybersecurity threats grow increasingly more complex and the consequences to American democracy and way of life become clearer, the need for a consolidated and harmonized approach to cybersecurity across all levels of the U.S. government, internationally, and with the private sector, becomes increasingly critical. Cyber silos in different federal agencies create a patchwork of disjointed cyber activities that confuse both industry and government, undermine accountability, and put citizens at greater risk.

A National Cyber Director within the Executive Office of the President would have the capacity to oversee and coordinate a federal government response against adversarial cyber operations, as well as formulate and maintain an international cyber strategy to respond to threats. A whole of government viewpoint would also enable this position to effectively plan response efforts and deploy federal cyber resources.

2. You speak in your written testimony about how essential Chief Information Security Officers (or similar positions) are to company leadership. Would establishment of a National Cyber Director through H.R. 7331 implement the best practices of the private sector to improve the functioning of the federal government? Why or why not?

Yes, the establishment of a National Cyber Director through H.R. 7331 would help implement the best practices of the private sector to improve the functioning of the federal government. Best practices in the private sector means Chief Information Security Officers and Chief Security Officers plan and execute whole-of-company defense processes and practices, are instrumental to understanding and managing enterprise risk in the technology era, and work at the intersection of business and technology. They are empowered by company leadership and regularly engage with the CEO, Board of Directors and/or an Audit and Risk Committee of the Board on the cyber health of the organization.

Similarly, the President needs a principal advisor for cybersecurity within the federal government. A National Cyber Director would fill a similar role, with visibility into all the programs, systems and processes required for threat detection and prevention as well as business continuity and disaster recovery. This role will also lead the development of cybersecurity strategy and policy in coordination with federal agencies, conduct oversight of federal agency implementation of national and international cyber strategies, and make recommendations to the Office of Management and Budget on federal agency cybersecurity budget requests. The NCD will need to coordinate cyber activities across industries in the private sector and should have experience working with private industry and knowledge of their best practices and how interagency processes work.

In the private sector, organizations that prioritize cybersecurity do better – they're less prone to breaches, both small and large, that cause real impacts to their operations. This is true of the public sector as well. The better the federal government does cybersecurity and the more best practices they can implement, including those from the private sector, the more secure we will be, particularly as it relates to the convergence of information technology (IT) and operational technology (OT) infrastructures, both small and large, that cause real impacts to their operations.

3. H.R. 7331 requires the Office of the National Cyber Director to consult with private sector stakeholders on developing relevant operational or response plans to substantial cyberattacks, on emerging technologies, and on cybersecurity issues more generally. How would the National Cyber Strategy and federal cybersecurity posture be improved through consultation with the private sector as required in H.R. 7331?

The National Cyber Strategy and federal cybersecurity posture must be developed in consultation with the private sector because the majority of our nation's critical infrastructure is owned and operated by the private sector. National cybersecurity cuts across both private and public sector networks. Private sector stakeholders can bring front-line experience and expertise to cybersecurity strategy development processes. Private sector actors are also generally early adopters of emerging technologies. Improving national cybersecurity, therefore, requires effective consultation with the private sector to develop operational and response plans for substantial cyberattacks, as well as plans to help manage emerging technologies.

4. Your written testimony and our dialogue during the hearing addressed the lack of diversity in the cybersecurity sector and how it contributes to the overall shortage of talent in the cybersecurity workforce, indicating that "the nation needs a bold, new cyber workforce strategy that develops and advances the ranks of people from all walks of life." For example, you point out that minorities make up 26% of the U.S. cybersecurity workforce, and that women make up just 14% of the cybersecurity workforce in North America.

a. **Can you provide additional detail on what this strategy should include?**

Success in cybersecurity demands a multipronged approach that relies upon a diverse view of the problem. Simply put, diversity of thought, as well as racial and gender diversity, make our industry stronger.

While the private sector can lead the way, we need buy-in and partnership from the government to invest in recruiting, developing and retaining talent. Rob Joyce, Senior Cybersecurity Advisor to the Director of NSA, noted that we need to make systemic changes that address the cybersecurity skills gap and encourage the next generation of diverse cybersecurity professionals. An influx of cybersecurity talent is important in tackling the ever-expanding attack surface and threat landscape. If we're going to be successful and close the cyber exposure gap, increasing diversity must be a priority.

Congress should use its power to improve federal job preparedness programs and provide funding to help advance our competitiveness on a global scale. For example, Rep. Jim Langevin's Cybersecurity Skills Integration Act (H.R. 1592) would help prioritize the key skills needed for cybersecurity professionals to effectively protect our critical infrastructure. This bill would help retool our workforce to identify new threats posed to traditional IT environments via the new elastic attack surface in areas like internet of things (IoT), operational technology (OT), cloud and mobile.

b. Do you believe such an effort would advance innovation and give the U.S. a competitive edge globally?

Yes, diversity in cybersecurity is a must-have, and success in cybersecurity demands a multipronged approach that relies upon a diverse view of the problem.

Research from Dalberg revealed that "If two companies are identical in every way except for racial/ethnic diversity and female representation in leadership, the more diverse company will, in all likelihood, have higher revenues, be more profitable, and have a higher market value."

Numerous other studies have shown that more diverse teams are smarter, more innovative and more financially successful. Increasing diversity is key to unlocking the full potential of any organization and filling these critical roles. Committing to diversity in cybersecurity – bringing more women, minorities and diverse backgrounds is critical to maintaining U.S. leadership in the cyber and tech industry.

c. Do you think such a strategy should be included in the National Cyber Strategy?

Yes, a cyber workforce strategy regarding diversity should absolutely be a priority for the National Cyber Strategy and the National Cyber Director. Cyber workforce development requires top-level attention and should be at the forefront of priority initiatives for the National Cyber Strategy and the National Cyber Director to ensure that the U.S. remains competitive for the best cyber talent.

Only through increased inclusion and diversity—of race, gender, perspective and thought—can our industry achieve greater creativity and innovation and develop new solutions to our most vexing challenges. We need a whole-of-nation approach to addressing the lack of diversity in the cybersecurity sector. Companies across the country are making important progress, but we need buy-in and partnership from the federal government.

5. Do you think that most Americans are aware of the cyberthreat exposure they face daily, and how would H.R. 7331 reduce this exposure? What are the potential risks to Americans if commonly used apps, sites, and devices lack the infrastructure or ability to keep up with evolving cyberthreats, and how are those risks compounded if we fail to establish a centralized federal response?

No, I do not think that most Americans are aware of the cyberthreat they face daily. The 2020 Unisys Security Index surveyed more than 15,000 consumers and found "[m]ore than two in three Americans are not concerned about internet security despite a massive spike in cyber activity targeting people working remotely due to the coronavirus." The report also found that "70% of Americans said they were not concerned about their data security or being scammed while working from home, even as the Federal Trade Commission reported 52,000 new online fraud cases and the FBI disclosed a 400% increase in online crimes reported to its Internet Crime Complaint Center."

The cyber threats that Americans face today are far greater in scope and scale than a decade ago. By connecting devices to the Internet, using common apps, accessing websites, and utilizing cloud computing, among other things, Americans are increasing their overall cybersecurity attack surface and their risk of a cyberattack. Cyberattacks come in a variety of forms and can have a range of impacts, such as harming devices, compromising personal data, limiting the availability of data, and/or precluding the operation of critical assets.

However, as I referenced in my testimony, the vast majority of cyberattacks leverage unpatched, known vulnerabilities. Government policy should not allow for "learned helplessness" by federal government agencies or private industry. Helplessness allows individuals and organizations to remain negligent and avoid accountability for not taking even the most basic steps to improve cyber posture.

On the contrary, government policy should raise the bar for baseline cyber hygiene practices in both the public and private sectors. While the government can play a stronger role in deterrence, including thoughtful consideration of offensive capabilities, attributing attacks and establishing sanctions regimes, those efforts should not replace the promotion and implementation of basic cyber hygiene practices and processes.

A National Cyber Director with visibility across the whole of government would be able to apply a similar discipline across the federal government. Currently, the federal government's ability to protect its citizens and respond to these threats is hindered by a patchwork of disjointed cyber activities and approaches. Cyber responsibilities and capabilities are spread across various agencies that often operate in silos, and this undermines accountability and puts citizens at risk. Further, state and local government coffers are unable to spare funds to bolster cybersecurity amid a public health crisis.

H.R. 7331 would reduce this exposure through the creation of a National Cyber Director to lead a whole-of-government approach to develop cybersecurity strategies and policies in coordination with federal agencies; conduct oversight of federal agency implementation of national and international cyber strategies; make recommendations to the Office of Management and Budget on federal agency cybersecurity budget requests; and coordinate cyber activities across

industries in the private sector. This would certainly help to reduce the cyber exposure of Americans.

There are steps we can take to protect ourselves—as individuals, as organizations, and as a nation. The Director would help ensure that the government holds itself and industry accountable to achieve those steps to accurately protect the safety of all Americans.

6. You mentioned that "a modest amount of funding, coordination, and policy directed from the federal government [to state and local governments] could have a disproportionately huge impact on better protecting the nation" from cyberthreats." How would you design such a program?

First and foremost, I recommend we continue to support federal cybersecurity programs that focus on getting the basics right. Requiring federal agencies to maintain good cyber hygiene, built upon a robust vulnerability and threat management platform, goes a long way in protecting and maintaining IT systems and devices appropriately and executing cybersecurity best practices.

The federal government must also incorporate operational technology (OT) and the expanded attack surface into all of its cybersecurity programs. The vast infrastructure of OT makes everyday activities – turning on lights, running water, charging devices – increasingly exposed to serious cyber threats. Bad actors and foreign state actors know how much we rely on this critical infrastructure and are more than happy to exploit that reliance. There is an increased focus on OT security across the cyber industry, and the federal government has an important role to play in OT security. Effectively securing the nation's OT will take a collaborative, whole-of-government partnership with industry.

###

QUESTIONS FOR THE RECORD
On behalf of Ranking Member James Comer (R-KY)
Committee on Oversight & Reform
"U.S. Cybersecurity Preparedness and H.R. 7331, the National Cyber Director Act"
Hearing took place on Wednesday, July 15, 2020, remotely via Webex

---

Questions for Mr. Amit Yoran:

1. "Hack back" legislation has been proposed in Congress. Private industry would be offered the authority to respond in kind if a company becomes the target of a cyber-attack. Do you support such legislation?

No, I do not support "hack back" legislation. First, most companies lack the skills needed to take on the often-sophisticated groups behind cyberattacks. With criminal groups and even nation-states behind many cyberattacks, allowing private companies with small cyber teams to respond to a nation-state is a recipe for disaster that could lead to much larger global conflicts that could quickly move outside cyberspace.

Second, attribution is incredibly difficult in cyberattacks. Hackers can spoof their IP addresses or use another group's signature tools, making it difficult for governments, let alone private companies, to accurately identify and respond to a hack. Simply put, the chances of a private company responding to a cyberattack by hacking the wrong group, or even nation-state, is significant, and hack back legislation provides no protection to these companies for when things go wrong.

Finally, Federal Bureau of Investigation Director Christopher Wray has indicated the FBI does not support hacking back. At a Council on Foreign Relations event in April 2019, Director Wray stated, "We don't think it's a good idea for private industry to take it upon themselves to retaliate by hacking back at somebody who hacked them. That creates all kinds of potentially unintended consequences. And so not something we would recommend, any more than we would recommend people taking justice into their own hands privately in another arena."

2. Could you please describe a hypothetical situation that sufficiently characterizes the cyber threats posed to industrial control systems security and how those threats can be remediated?

Operational Technologies (OT) used in critical infrastructure, manufacturing, pharmaceutical, building automation, etc. environments are increasingly connected through intentional or accidental convergence with information technology (IT) and these systems can no longer be considered separated by the mythical air-gap.

Many cyber threats to these systems exist ranging from nation states, criminals, malicious insiders and other miscreants seeking to do harm to these systems. The adversary's objectives could be intellectual property theft, reconnaissance for future targeting, ransomware for monetary gain or actual physical damage.

What differentiates the severity of an attack against an industrial control system (ICS) versus an attack on IT or an enterprise system is the consequence of a successful attack. IT system intrusions are mainly focused on the loss of personally identifiable information such as credit card numbers, whereas an attack on ICS can impact the safety and reliability of our critical national infrastructures, in fact putting American lives at risk.

Unfortunately, we don't need hypothetical scenarios to demonstrate this threat and the resulting damage a successful cyberattack could inflict on our critical infrastructure as evidenced by the recent National Security Agency (NSA)/Cyber Infrastructure Security Agency's (CISA) advisory which warned of recent malicious activity targeting operational technology and critical infrastructure.[1] In addition, the Department of Homeland Security (DHS) and the CISA's control systems team has published many alerts over the years documenting this existential threat to our critical infrastructure.[2]

One Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) alert focused on the BlackEnergy malware campaign that resulted in electricity outages to customers in Ukraine and compromised numerous other ICSs environments.[3] Malware such as this can leverage known vulnerabilities in the devices and systems that make up the OT and ICS environment. Once an adversary has successfully compromised these networks, they literally can take full control of the systems to accomplish their specific objectives.

The good news is that the OT and ICS cybersecurity field has matured over the past decade and solutions are available to assist critical infrastructure operators in monitoring the cyber health of these systems in real-time. The ability to understand what devices and assets are connected to these networks and to subsequently prioritize mitigation and remediation efforts are currently available as off-the-shelf products for purchase.

We would urge Congress to consider language requiring that critical national infrastructures have these most basic of cyber hygiene practices in place.

3. If you had the power to immediately require the U.S. government to focus in on one specific component of cybersecurity, what would it be?

First and foremost, we must get the cybersecurity basics right. Requiring federal agencies to maintain good cyber hygiene, built upon a robust vulnerability and threat management platform, goes a long way in protecting and maintaining IT systems and devices appropriately and executing cybersecurity best practices.

However, the U.S. government needs to also ensure it incorporates operational technology (OT) and the expanded attack surface into all of its cybersecurity programs. The vast infrastructure of OT makes everyday activities – turning on lights, running water, charging devices – increasingly

---

[1] U.S. CERT, "NSA and CISA Recommend Immediate Actions to Reduce Exposure Across Operational Technologies and Control Systems," *https://us-cert.cisa.gov/ncas/alerts/aa20-205a*

[2] ICS-CERT Alerts, https://us-cert.cisa.gov/ics/alerts

[3] U.S. CERT, "Ongoing Sophisticated Malware Campaign Compromising ICS (Update E)", https://us-cert.cisa.gov/ics/alerts/ICS-ALERT-14-281-01B

exposed to serious cyber threats. Bad actors and foreign state actors know how much we rely on this critical infrastructure and are more than happy to exploit that reliance. There is an increased focus on OT security across the cyber industry, and the federal government has an important role to play in OT security. Effectively securing the nation's OT will take a collaborative, whole-of-government partnership with industry.

###