Written Testimony
Amit Yoran
Chairman and CEO, Tenable, Inc.
House Committee on Homeland Security
“Hearing on Mobilizing our Cyber Defenses: Securing Critical Infrastructure Against Russian Cyber Threats”
March 30, 2022

Introduction

Chairman Thompson, Ranking Member Katko, and members of the Committee, thank you for the opportunity to testify today on securing our critical infrastructure against Russian cyberthreats. We are at a major inflection point in history and how we respond will make all the difference. Thank you for your leadership always, and particularly at this incredibly important time.

My name is Amit Yoran and I am the chairman and CEO of Tenable. I have spent more than 20 years in the cybersecurity field, both as a public servant and in industry. I earned a master’s in computer science from The George Washington University and a bachelor’s in computer science from the United States Military Academy. I served as the director of the National Cybersecurity Division and as the founding director of the United States Computer Emergency Readiness Team (US-CERT) program. Additionally, I have served on a number of Presidential advisory commissions. As an innovator and entrepreneur in the security space, I founded and built two security companies: Riptech, acquired by Symantec; and NetWitness, from which I went on to serve as the president of RSA after it acquired NetWitness. I have also served as a director and advisor to security startups and industry advisory boards. I have previously testified before congressional committees on cybersecurity policy, encryption and other related issues.

The company I lead, Tenable, is headquartered in Columbia, Maryland. Tenable has over 1,600 employees globally and more than 40,000 customers worldwide. Tenable is publicly traded on the NASDAQ and is the world’s leading provider of vulnerability management capabilities. Our company provides organizations with an unmatched breadth of visibility and depth of analytics to measure and communicate cyber risk. We believe cybersecurity is foundational to making better and more strategic decisions. Our goal is to eliminate blind spots and help organizations prioritize which actions they can take to most efficiently reduce exposure and loss.

Simply put, Tenable empowers organizations of all sizes to understand and reduce their cyber risk. For the federal government specifically, Tenable provides the most widely deployed vulnerability assessment solution, serving just about every department and agency. Our solutions are also broadly used by state and local governments to manage cyber risk.

Understanding the Threat

Knowing what the threat is, the impact it could have on your systems and how to respond is far more important than knowing where the threat is coming from.

Understanding where the threat is coming from is useful from the perspective of national cyber strategy, defense and intelligence. It can also help determine how to prioritize remediations based on the motivations of threat actors. Beyond that, knowing where a threat is coming from has little impact on how an organization responds. For almost all organizations, cybersecurity risk management practices are the same regardless of whether the attack is coming from the Russians, other nation states, cyber criminals or other bad actors.

Ransomware against critical infrastructure providers is incredibly profitable for cybercriminals, as demonstrated by the Conti ransomware data leaks. The Conti group and its affiliates reportedly made use of over 30 known vulnerabilities, some of which were first disclosed in 2018. The Conti bitcoin wallet data showed more than $1 billion had been paid, creating a massive funding method for Russian actors. Ransomware is also a very flexible weapon, as demonstrated by the Russian-attributed malware BlackEnergy and CrashOverride, both of which were used in attacks against the Ukrainian power grid, and were very sophisticated and modular with payloads that could be delivered in near real-time to the victim. Two separate indictments from the Department of Justice (DOJ) were unsealed on March 25, charging four Russian nationals for extensive hacking campaigns against critical infrastructure providers worldwide.[1]

LAPSUS$ has shown that with only $25,000, a group of teenagers could gain access into organizations that have even the most mature security practices. The thought of a **nation state — with much deeper pockets, focus, patience and a mission — targeting these sectors should be a sobering, if not terrifying, call to urgent action.**

The State of U.S. Critical Infrastructure

Last week, President Biden warned of the potential for Russian cyberattacks against the United States in response to the economic costs we have imposed following the invasion of Ukraine. He urged governors, private sector partners and critical infrastructure providers to harden their cyber defenses immediately. The White House also issued a Fact Sheet, "Act Now to Protect Against Potential Cyberattacks," that called for companies to deploy multi-factor authentication, continuous monitoring and threat mitigation, to make sure systems are patched and protected against all known vulnerabilities, build security into products from the ground up, and use modern tools to check for known and potential vulnerabilities.

Critical infrastructure is not one thing, and most critical infrastructure industries vastly differ. The Cybersecurity and Infrastructure Security Agency (CISA) has identified 16 critical infrastructure sectors in the U.S., including financial services, energy providers, water and wastewater treatment facilities, and transportation systems. There is no singular defense paradigm that could effectively be applied across all the sectors. Some critical infrastructure providers have a high degree of cybersecurity preparedness, strong risk understanding and risk management practices, and very strong security programs. Others are woefully ill prepared.

All critical infrastructure sectors continue to undergo digital transformation, resulting in an expanding cyberattack surface. New technology investments represent great efficiency opportunities, like the move to smart factories and smart cities, but these shifts can introduce real gaps in security. Without

[1] TechTarget, "US indicts Russian nationals for critical infrastructure attacks," https://www.techtarget.com/searchsecurity/news/252515161/US-indicts-Russian-nationals-for-critical-infrastructure-attacks

enhancements to security and resiliency, critical infrastructure providers are left unprepared to address cyberthreats.

Just this week, a new report from the Center for Strategic and International Studies (CSIS) and Trellix, yet again, put this lack of preparedness in writing. The report, based on survey results from 800 IT decision makers from several countries around the world, including the United States, found that 9% of critical infrastructure operators don't even have a cybersecurity strategy in place, despite the fact that 85% of respondents believe they have been targeted by a nation-state cyberthreat.

Certain critical infrastructure sectors better understand strategic risk assessments and cyber risk management as a discipline. Generally speaking, the cybersecurity practices in these markets and industries have been more highly regulated than others.

For example, the financial services sector has long relied on IT and has built strong cyber risk management processes and practices. Most modern banks realize that, in many ways, they are technology companies. For decades, everything from bank accounts to transactions to data analytics have been digitized, resulting in a culture of strong security practices. These security practices have been encouraged through a high level of regulation and oversight. While dramatic differences can be found in the security readiness of individual banks, the sector as a whole has strong security and is resilient as a critical infrastructure.

For years, the electric industry operated on voluntary compliance of reliability standards, but following the Northeast blackout of 2003, Congress authorized the mandatory development of reliability standards, which included cybersecurity (Energy Policy Act of 2005).

Due, in part, to regulation by the Federal Energy Regulatory Commission (FERC), which oversees the reliable operation of the bulk power system, the electric sector has improved cyber resiliency. FERC certified the North American Electric Reliability Corporation (NERC) to oversee electric reliability, and as part of its definition of resilience, included cybersecurity as critical. Today, cybersecurity standards in the energy sector continue to be developed and enforced by NERC resulting in improved security and reliability.

As IT and operational technology (OT) systems become increasingly interconnected, even some well managed critical infrastructure sectors remain at risk**.** For example, some industries, such as mining, chemical plants and fuel pipelines, already have safety systems to prevent destruction of physical infrastructure and bodily harm or loss of life. However, as organizations increasingly interconnect their IT and OT systems in the pursuit of improved efficiency, more control settings become digitized. As a result, the effectiveness of some of these safety measures may be brought into question.

On May 7, 2021, Colonial Pipeline was hit with a ransomware attack that caused the company to shut its operations for six days, prompting the President of the United States to issue a state of emergency. The compromise affected billing systems responsible for tracking and invoicing the amount of fuel each distributor receives. These business systems were actually located in the organization's IT environment, not its OT environment. The OT systems that control the pipeline itself were not directly accessed in the attack. Yet, the fear and uncertainty of the possible reach of the attack contributed to Colonial Pipeline's decision to shut down pipeline operations. Colonial Pipeline ultimately ended up paying the hacking group DarkSide a total of 75 bitcoins ($4.4 million) for the ability to unlock its systems and get fuel back out to a majority of the East Coast. This highly visible incident serves as a stark example of the potential negative impact of increasing IT/OT convergence.

The Colonial Pipeline incident also highlights the importance of maintaining cyber hygiene. The attack vector in this case was the cracking of a password for an account no longer in use, that had remote access to the corporate network. Enabling multi-factor authentication and disabling dormant accounts are simple but effective examples of things that need to be done methodically and rigorously to reduce exposure.

Other critical infrastructure sectors have not prioritized cyber and are largely blindsided by cyber as a strategic risk. Some of these sectors haven't historically thought of interconnectivity, access, complexity and digitization as strategic cyber risk and haven't been regulated in that way.

For example, many healthcare providers and hospitals have long viewed IT as a cost efficiency play for automation and sharing information when needed to provide better care, not necessarily a strategic asset. Consequently, attackers have caught many healthcare organizations off guard.

Ransomware attacks on the healthcare sector have demonstrated its susceptibility to cyberattacks and have often exposed poor cyber hygiene practices. WannaCry, which took advantage of a well-known vulnerability for which patches were widely available and broadly distributed, shut down hospitals around the world. Even though medical equipment was still operating, hospitals couldn't onboard new patients or use their systems to track the distribution of medicines. Just last year, Scripps Healthcare, a non-profit healthcare organization with five hospitals and 19 outpatient facilities in Southern California, was hit with a ransomware attack that impacted critical IT and backup systems. Scripps was forced to reroute stroke and heart attack patients to other facilities, an impact that could have cost lives. The company lost nearly $113 million as an immediate result of the attack, and now faces a class action lawsuit due to the medical records of nearly 150,000 patients being exposed.

While the Scripps example is a costly one, it is but one example of how much ransomware attacks are costing our medical industry. If we look at the number of ransomware attacks across the healthcare industry alone in 2020, combining the ransoms paid and the amount of downtime tracked, there was a loss of $20.8 billion. This is double what it was in 2019 and 10 times more than in 2018.[2]

A closer look at the data reveals stark differences among critical infrastructure sectors. According to Tenable's own vulnerability data, financial services organizations and organizations in the energy sector, which encompasses more than the electric sector, average about the same number of critical vulnerabilities per device, showing a relative approximation in the maturity of their cyber practices. Contrast that with healthcare and manufacturing, which average twice as many critical vulnerabilities per device. The median time for financial services and energy sector organizations to remediate a critical vulnerability is approximately 12 days, while manufacturing and healthcare average 29 and 32 days,

[2] HIPPA Journal, "Scripps Health Ransomware Attack Cost Increases to Almost $113 Million," https://www.hipaajournal.com/scripps-health-ransomware-attack-cost-113-million/;
GovInfoSecurity, "Scripps Health Reports Financial Toll of Ransomware Attack," https://www.govinfosecurity.com/scripps-health-reports-financial-toll-ransomware-attack-a-17288;
Comparitech, "Ransomware attacks on US healthcare organizations cost $20.8bn in 2020," https://www.comparitech.com/blog/information-security/ransomware-attacks-hospitals-data/#How_much_did_these_ransomware_attacks_cost_healthcare_organizations_in_2020

respectively. This gap provides adversaries ample opportunity and highlights the sample disparities in the cyber maturity of these sectors.

There are also vast disparities in the amount of funding available to critical infrastructure providers. Many systems run by municipalities, such as **water and wastewater**, do not have the same funding or cybersecurity expertise to combat the evolving threats. In February 2021, a water treatment plant was breached in Oldsmar, Florida, a town of 15,000. The attacker attempted to change the alkaline levels in the water to a level that would severely damage human tissue. It's another striking example of the risks of IT/OT convergence; the attacker gained access to a remote IT management software called Team Viewer, and from there "accessed the system by exploiting cybersecurity weaknesses including poor password security, and an outdated Windows 7 operating system," according to the FBI. This attack further demonstrates the significance of proper system hygiene.[3]

Some critical infrastructure sectors, including the energy sector's oil and gas refining and extraction industries, are still largely unregulated when it comes to cybersecurity, and that is a particularly concerning scenario when we consider that those critical systems are frequently managed using workstations running on outdated operating systems and software. It's worth noting that pipeline owners and operators are now subject to new baseline cybersecurity standards through a TSA Directive,[4] however the rest of the sector remains largely unregulated.

Rapid Connectivity and the Risks of IT/OT Convergence

A recent assessment of an available search engine for internet connected devices revealed that more than 28,000 Industrial Control Systems (ICS) and Supervisory Control and Data Acquisition (SCADA) systems are directly accessible from the internet.[5] While not directly accessible from the Internet, countless more can be accessed via increasingly popular service portals, which can themselves be compromised. Combine that with human error and frequency of poorly configured software, and the rapid connectivity required to keep today's OT environments running efficiently, we may be entering an era which exponentially hastens systemic cybersecurity failures. Systems that are interconnected in ways they weren't designed leads to complexity and breeds insecurity.

These systems, and other OT technologies used in critical infrastructure environments, are notoriously difficult to patch because systems may have to be taken down and thoroughly tested each time an update is made. Existing operating models for most OT environments, such as power plants, gas pipelines and manufacturing plants, leave little margin for downtime. These companies have historically tried to reduce their exposure by highly segmenting their environments, but the increase of IT/OT convergence is making segmentation less effective, resulting in systems that can't be patched or secured as targets.

[3] ABC News WFTS Tampa Bay, "FBI: Water system hack likely caused by remote access program, old software and poor password security," https://www.abcactionnews.com/news/local-news/i-team-investigates/fbi-water-system-hack-likely-caused-by-remote-access-program-old-software-and-poor-password-security;
Wired, "A Hacker Tried to Poison a Florida City's Water Supply, Officials Say," https://www.wired.com/story/oldsmar-florida-water-utility-hack/

[4] U.S. Department of Homeland Security, "DHS Announces New Cybersecurity Requirements for Critical Pipeline Owners and Operators," https://www.dhs.gov/news/2021/05/27/dhs-announces-new-cybersecurity-requirements-critical-pipeline-owners-and-operators

[5] Shodan, https://www.shodan.io/

Furthermore, many critical infrastructure organizations still fail to segment their IT and OT environments. There are increasingly compelling business reasons to create interconnection points between these environments, but doing so without an appreciation of the consequences such actions represent can result in system risks which are not understood.

What Can Critical Infrastructure Providers Do?

Critical infrastructure providers have a duty of care, highlighted in turbulent times, to be responsible stewards of the services that are relied on by millions of Americans. Protecting ourselves means knowing what's on your network and maintaining it in good working order, which includes protecting against known vulnerabilities.

As more people have access to these systems, security quickly breaks down unless tight identity management practices are in place. Systems must be treated as if a sophisticated adversary already has or can gain access.

CISA released insightful guidance on recommended practices that organizations can take to best prepare themselves from a cyber perspective. Some of these practices include:

- **Asset Inventory and Risk Characterization.** The foundation for every security framework, whether IT or OT, always begins with visibility into the assets for which you are responsible. It is critically important to be able to understand the network layout of your environments, the systems that reside in those networks, the software installed, how they are configured, how they are accessed, and the function they serve to the mission of the organization. Only when you have this level of visibility can you begin to quantify the risk profile of these environments and a strategy to secure it.

- **Vulnerability and Patch Management Program.** It is important for every organization to follow a well-defined vulnerability and configuration management program that is able to not only identify Common Vulnerabilities and Exposures (CVEs) in the environment, but also identify how these critical systems are configured and identify when those configurations change. They also need well defined processes in place to remediate issues identified through patch and configuration management programs that take into account the complexities of the systems running and the importance they play to the organization.

- **Network Segmentation and Remote Access.** Historically, OT systems have been completely separated from other environments. With the convergence of IT/OT systems, this practice is increasingly untenable and frequently violated. Whether it is Active Directory trusts between corporate and OT domains, or remote access being granted to enable remote access for monitoring or troubleshooting purposes, interconnectivity of systems is already today's reality. A continual audit of access and interconnectivity into these environments is an absolute imperative, and that includes assessing and monitoring the integrity of the Active Directory and other access control systems. Who is allowed to connect to them and the hygiene of the systems that are connecting are foundational to understanding the integrity of and risk to critical infrastructures.

- **Cybersecurity Training/Education on OT.** Because OT environments have historically been separated from everything else, the notion of securing them is relatively new for both IT personnel as well as OT engineers. Training must be mandatory for OT engineers, who have typically not had to consider the cyber risks their actions or inactions might introduce. IT security teams in these organizations must also undergo training to better understand the ways that OT systems differ from IT, and the unique challenges associated with securing critical infrastructure.

How Can the Government Help Industry?

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. Government can surely play a stronger role in deterrence, to include thoughtful consideration of offensive capabilities, attributing attacks and establishing retorts and countermeasures as appropriate; however, those efforts should not replace strong basic cyber hygiene practices.

Tenable recommends the following steps that government should implement to enhance the cyber preparedness of U.S. critical infrastructure:

- **Establish baseline cybersecurity standards of care for critical infrastructure that align with international standards and the National Institutes of Standards and Technology (NIST) Cybersecurity Framework, based on effective cyber hygiene practices.** Basic cyber hygiene for critical infrastructure operators includes continuous understanding of what assets are on your network, ensuring strong identity and access management, scanning for and patching known vulnerabilities, and implementing incident detection and response capabilities.

- **Finalize and implement the proposed SEC rule that requires public companies to disclose their policies and practices to address their cybersecurity risks.** The SEC's Proposed Rule on Cybersecurity Risk Management, Strategy, Governance and Disclosure would require public companies to disclose their policies and procedures for identifying and managing cybersecurity risks, management's role in implementing cyber policies and procedures, and the board of directors' cybersecurity expertise.[6] This is the single action that would most dramatically improve our cybersecurity preparedness as a nation. Requiring greater transparency of cyber risk practices and oversight forces companies to treat cybersecurity risk as a business risk and will lead to stronger cybersecurity governance and accountability among corporate leaders and boards, and ultimately more effective cybersecurity practices.

  Cybersecurity breaches can damage a company's financial condition. In addition to the costs of remediation from a cyberattack and loss of customers, revenue and reputation, there are risks of shareholder lawsuits, customer lawsuits, increases in insurance premiums and increased scrutiny from external auditors and the board of directors. There are indirect consequences to cyber failures as well; cyberattacks can distract management, resulting in new problems; they can also trigger customer audits of a company's cybersecurity defenses, which can lead to the

[6] Cyberspace Solarium Commission, Final Report, https://www.solarium.gov/report

involvement of outside counsel and other third parties, and significant added expenses.[7] In forcing corporate leadership to pay attention, this proposal serves as the most significant driver for companies to establish baseline cybersecurity practices and processes.

- **Implement the cyber incident reporting requirements included in the FY 2022 Omnibus Appropriations bill.** CISA must implement these new requirements in a way that will enable actionable incident information to be shared with owners and operators of critical infrastructure systems so that they can take steps to protect themselves and seek to mitigate any ongoing attacks.

- **Support and strengthen value added engagement between the private sector and public sector**. The JCDC, of which Tenable is a member, is bringing together representatives from private industry and key government agencies to drive strategic planning and incident response capabilities. This type of operational government-industry engagement has been a positive step forward, and we thank CISA and Director Jen Easterly for their continued support and urge them to continue strengthening the JCDC's alignment.

  In response to the ongoing Russia-Ukraine conflict, CISA established its Shields Up initiative to encourage all organizations to adopt a heightened posture of vigilance. Shields Up has developed helpful resources to empower organizations to prepare for and defend against cyberattacks.

Protecting Government Networks and Systems

- **Accelerate effective Zero Trust implementation by federal agencies**. Congress should provide federal agencies with the resources needed to implement Cyber Executive Order 14028 to modernize and strengthen our collective cyber defenses, recognizing that Zero Trust is a philosophy that dictates systems design and operation, not a singular product.

- **Strengthen government networks by including protection of federal OT and Active Directory services in the Continuous Diagnostics and Mitigation (CDM) Program.**
  - **OT:** Federal civilian agencies own and operate a multitude of OT and ICS, particularly through the Departments of Energy and Commerce. However, the government doesn't currently have a firm grasp of all the assets it controls. By adding OT/ICS security to the CDM program, government agencies will be required to conduct an inventory of their OT/ICS systems, and to take steps to strengthen their security.
  - **Active Directory.** Active Directory is one of, if not the most highly targeted and compromised pieces of infrastructure. These systems provide access control across the network and persistence should attacks be detected. As highlighted by the Mandiant breach disclosures, Russian and other foreign intelligence services are actively targeting Active Directory when going after US Government systems. All government systems must incorporate Active Directory security to ensure least privileges for user identities, and to scan for misconfigurations that can be exploited to gain access to Active

[7] Harvard Business Review, "The SEC Is Serious About Cybersecurity. Is Your Company?" https://hbr.org/2021/09/the-sec-is-serious-about-cybersecurity-is-your-company

Directory and monitor for ongoing suspicious and high-risk activities within Active Directory.[8]

- **Implement Section 1505 of the FY 2022 National Defense Authorization Act**. This provision requires the Department of Defense to conduct an inventory of OT assets and update its policies to establish baseline cybersecurity requirements for operational technology.

- **Establish metrics for transparency and accountability.** Congress should update its oversight of agency cybersecurity by using the Federal Information Technology Acquisition Reform Act as a model to replace existing unstructured agency reporting. A cybersecurity scorecard would provide improved transparency metrics and milestones against which all agencies measure and report their progress.[9]

- **Ensure sufficient funding for CISA and the Office of the National Cyber Director to ensure they can meet mission requirements.** I supported the creation of the Office of the National Cyber Director and applaud Director Chris Inglis' efforts to stand up and staff the new office. The threats to federal networks and critical infrastructure are growing at a significant rate, and CISA must serve as an effective coordinator to strengthen security in these environments. Congress should see the FY 2022 appropriations for CISA as a new baseline number, which should grow at a rate commensurate with the needs of the mission.

Conclusion

There are fundamental steps all providers must take, from knowing what's on their network and how those systems are vulnerable to addressing those exposures, and from controlling user access and privileges to managing critical systems that are interconnected, that will make it harder for bad actors to compromise critical infrastructures.

Many critical operating environments lack a formal systemic approach to risk assessments and processes, let alone the continuous visibility expected for critical services and high value targets. These formal processes are desperately needed as rapid increases in access and interconnectivity dramatically increase risk**.** In these instances, regulation for transparency and standards of care can help drive improvement in risk management practices and at the same time foster innovation.

I would like to thank Chairman Thompson, Ranking Member Katko and all the members of the Committee for your attention to this important issue. I appreciate the opportunity to testify today and look forward to working with you and your colleagues as we collectively mobilize our cyber defenses.

[8] U.S Department of Commerce, "NOAA Inadequately Managed Its Active Directories That Support Critical Missions," https://www.oig.doc.gov/OIGPublications/OIG-22-018-A.pdf

[9] MITRE, "Eight Recommendation for Congress to Improve Federal Cybersecurity," https://www.mitre.org/sites/default/files/publications/pr-21-3403-eight-recommendations-for-congress-to-improve-federal-cybersecurity.pdf