Written Testimony of Jim Richberg

Head of Cyber Policy & Global Field CISO

Fortinet, Inc.

Before the U.S. House Committee on Energy & Commerce

Subcommittee on Communications and Technology

Hearing on “Safeguarding Americans' Communications:

Strengthening Cybersecurity in a Digital Era“

January 11, 2024

899 Kifer Road
Sunnyvale, CA 94086

Tel: +1-408-235-7700
Fax: +1-408-235-7737

www.fortinet.com

Chairman Latta, Ranking Member Matsui, Chairwoman McMorris Rodgers, Ranking Member Pallone, and distinguished members of the Subcommittee, I appreciate the opportunity to testify before you today on the growing importance of a strong national cyber posture to protect Americans' communications.

My name is Jim Richberg and I serve as Head of Cyber Policy and Global Field Chief Information Security Officer (CISO) at Fortinet.[1] Fortinet is a US company that is one of the largest cybersecurity companies in the world. While we manufacture over half of the firewalls sold worldwide, our portfolio actually extends across over 50 different and integrated cybersecurity and networking products and services, reflecting our commitment to innovation as information technology and cyber threats have continued to evolve. In addition to our products and services, Fortinet operates a robust cybersecurity training institute focused on closing the cyber workforce and skill gaps and creating a more digitally aware society.[2] We are also part of numerous collaborative activities between industry and the US Government, ranging from participation in the IT Sector Coordinating Council to collaboration on technology development through NIST's National Cybersecurity Excellence Partnership (NCEP) and coordinated cyber threat analysis and response via the Joint Cyber Defense Collaborative (JCDC) established by CISA. Reflecting the fact that cybercrime does not stop at country borders, Fortinet also participates in global initiatives such as the World Economic Forum Centre for Cybersecurity and the Cyber Threat Alliance.[3]

I represent Fortinet on multiple public-private sector councils and work with governments and large enterprises across the US and globally to address complex cyber problems ranging from Artificial Intelligence (AI) to Zero Trust. My knowledge of cybersecurity, the cyber threat landscape, and the need for building cyber resilience within organizations and nationally is based upon my 33 years of service in the U.S. Government as well as my work at Fortinet. I oversaw the implementation of the whole of government Comprehensive National Cybersecurity Initiative (CNCI) for Presidents Bush and Obama and served as the National Intelligence Manager for Cyber for two Directors of National Intelligence. I was responsible for creating a unifying cyber strategy for the US Intelligence Community and for setting its cyber threat priorities.

[1] https://www.fortinet.com/corporate/about-us/about-us
[2] https://training.fortinet.com
[3] https://centres.weforum.org/centre-for-cybersecurity/

The Digital Environment

The technology environment we face today is different than it was when I retired from Federal service at the end of 2018. Among the technologies that have had the greatest impact in changing this environment are the migration from on-premises to cloud-based computing and storage, the growth in software-defined versus wired networks, expanded breadth and power of AI enabled services, and the proliferation of Internet of Things (IOT) devices. These technologies intersected with broader issues such as the COVID-fueled imperative to enable remote work and off-site connectivity, with the result that IT and communications are now focused on enabling the connection of users, devices, data, and computing power regardless of where any of these elements are located and how they are provisioned. This makes security more important than ever – and we are now seeing technologies and devices that provide both security and connectivity, as well as a broad evolution toward viewing security as an integral part of core business operations.

The concept of convergence is an increasingly important element of the technology landscape. It reflects convergence between networking and security, which are increasingly provided by products that perform both these functions and which in a growing number of organizations are managed by a unified networking and security team. Convergence also describes the fact that Operational Technology (OT) networks that once were "air-gapped" with their communications separate from the Internet and from corporate IT networks are, in many cases, now reachable from the Internet and connected to their business' IT networks. Fortinet's own research, informed by more than 550 OT security professionals around the globe, tells us three-fourths of OT organizations reported at least one intrusion in the last year and nearly one-third of respondents reported being victims of a ransomware attack.[4]

The concept of critical infrastructure is a way of characterizing the fact that compromise or successful cyber attack on certain organizations or networks has an effect that extends beyond the organization and its customers. The US Government designated 16 critical infrastructure sectors in 2013 and there have been efforts to designate a smaller set as 'lifeline critical infrastructure' or 'systemically important critical infrastructure' sectors. Communications is one of these core subsectors, as is energy generation and distribution because in the sustained

[4] https://www.fortinet.com/content/dam/fortinet/assets/reports/report-state-ot-cybersecurity.pdf

absence of power the operation of all other sectors and our daily lives as Americans is profoundly affected. Malicious cyber activity directed against the energy sector worldwide has grown rapidly in recent years, and we have seen cyber attacks with impact ranging from disabling remote controls for wind farms and disrupting use of prepaid electricity meters to data breaches that compromised customer names, addresses, and bank account information. There have also been high profile attacks on the communications sector including data breaches on customer information that resulted in exposure of their personal and financial information on the dark web.

Cyber Threats

The threats we face as individuals, organizations, and as a nation have continued to evolve along with technology. I spent much of my government career at the Central Intelligence Agency, but when talking about cyber threats we often refer to what I call *'the other CIA'* – threats to the confidentiality, integrity, or availability of information. In other words, actions to steal your data, manipulate or alter its content, or to prevent access to the data or to digital services. And while we often use the phrase 'cyber attack', most malicious cyber activity usually involves the theft of data rather than its destruction. You will also hear the phrase 'attack surface' used as a shorthand description of the increasingly complex digital environment – one in which it is difficult to know all the connection points and interactions between networks, devices, data, and users, much less to adequately defend them.

We often talk about "Advanced Persistent Threat" (APT) actors who are usually associated with nation states. These threats have tended to be more sophisticated and because they don't need to turn a profit – unlike criminals – they can be patient and persistent in targeting and penetrating would-be victims. Both nation states and criminals have overwhelmingly focused on stealing data, but they increasingly target its availability and sometimes delete or attack the data or the services it enables. Since I left Government perhaps the most significant change in threat activity has been the dramatic expansion of ransomware – malicious cyber activity that encrypts a victim's computers and renders the data inaccessible until a ransom is paid. Too often we see news reports of ransomware attacks across our economy including high profile attacks in the education, healthcare, and energy sectors. This type of malicious activity has been successful enough over time to fuel the growth of what Fortinet calls Advanced Persistent Crime – criminal

groups that coalesce and stay together, gaining sophistication and capability and blurring the traditional line between nation state and criminal activity.

We have also seen the emergence of trends in cyber threat activity that lower the barrier to entry by would-be cyber criminals. There is a robust marketplace in Ransomware-as-a-Service through which cyber criminals can rent malicious software and mount effective cyber attacks without having to know how to program or having technical insight into how target networks operate. The most common technique observed by Fortinet's threat researchers and analysts is for cyber criminals to gain access to their victims through compromised valid accounts and access credentials. Individuals or groups that specialize in acquiring and selling unauthorized access to computer systems and networks have emerged as a core part of the cybercriminal ecosystem, obviating the need for would-be threat actors to penetrate target networks from scratch.

The Human Element

At its core, cybersecurity is a team sport. The "human element" is an important part of the cybersecurity equation. We appreciate the Committee's focus on the importance of cyber awareness as building this requires a whole-of-society effort. At Fortinet we consider addressing the human element as part of our cybersecurity mission, helping build the cyber workforce of the future and ensuring that all members of society have cyber awareness and fundamental competence in cybersecurity.

To be successful, efforts with users need to begin at a young age and must involve partnerships across government industry and academia. To that end, Fortinet has invested heavily in the Fortinet Training Institute and has made significant commitments to this cause over the past 3 years.[5] In 2021 we committed to training over 1 million new users over five years to help close the sizeable cyber skills gap, and we are on track, having achieved over 43% of this goal by the end of 2023.[6] In 2022 we committed to offer free cyber awareness training to all K-12 faculty and staff in the U.S.[7] This program has reached over 350,000 users in more than 30 states. In

[5] https://training.fortinet.com/
[6] https://www.fortinet.com/corporate/about-us/newsroom/press-releases/2021/fortinet-pledges-train-1-million-people-help-close-cybersecurity-skills-gap-following-white-house-summit
[7] https://www.fortinet.com/corporate/about-us/newsroom/press-releases/2022/fortinet-announces-free-training-offering-schools-white-house-cyber-workforce-education-summit

2023 we expanded our support of the K-12 program to include free curriculum content for teachers to use in their lesson plans for K-12 level students.[8]

Key Areas for Action

From my experience both in Federal service and in the private sector, I would like to raise the following themes because I see them as important areas where the Committee is well positioned to drive progress.

Partnership

Effective cybersecurity requires partnership. Even the largest Federal agency or private sector company would be hard pressed to be fully self-sufficient in cybersecurity; and it needs capabilities, data, and services from others. This partnership is multidimensional and multidirectional, involving collaboration and a two-way flow of information between the public-private sectors, as well as within each sector. I elaborate on this theme in greater detail in some of the issues below.

Secure by Design

The US National Cyber Strategy released last year recognized that we need to increase our collective cyber resilience and identified the information technology sector as a key element for success because virtually every organization relies on commercial off-the-shelf IT and security products.[9] The Strategy identified the need to ensure that these products were "secure by design" with security included from the initial design phase, and that these products and services be delivered in configurations that are "secure by default" rather than expecting users, such as small businesses and individual citizens, to figure out how to enable the appropriate security settings and maintain them. Fortinet is proud to be one of the companies leading collaboration between the Federal government and industry to develop voluntary goals and approaches that will build our collective cyber resilience by ensuring that IT and communications products are secure by design and by default.

"Secure by design" and the impact of ensuring that security is considered as a design and

[8] https://www.fortinet.com/corporate/about-us/newsroom/press-releases/2023/fortinet-announces-free-security-awareness-curriculum-for-k-12-students-white-house-cyber-education-and-workforce-initiatives
[9] https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf

performance priority is relatively straightforward; “secure by default” is less intuitive, so I offer the following example. In many of the breach investigations conducted by Fortinet’s Incident Response team, the victim’s cybersecurity tools detected anomalous activity and generated alerts months before the full scale of the intrusion was realized and investigation began. Unfortunately, in many of these cases, the security tools were not configured by their users to save a copy of the suspect files, slowing detection and response.

Threat Intelligence

Cyber threat intelligence is essential because you can’t protect yourself against a threat that you don’t understand and therefore can’t detect. Cyber threat intelligence is generated in multiple forms and levels ranging from technical data that is machine generated and can be used in an automated fashion by cybersecurity tools to more strategic information that requires human analysis and interpretation. While the flow of tactical/technical information can be automated and is often provided automatically as a part of a cybersecurity product or service, the same is not true for more strategic level threat intelligence that requires skilled and scarce human talent to create and use.

Fortinet’s FortiGuard Labs uses one of the most effective and proven AI and ML systems in the industry to process and analyze data on billions of security events each day, sending actionable real-time threat intelligence to immediately increase customer defenses against threats, including novel (‘zero day’) exploits.[10] We believe that sharing intelligence and working with other industry partners, non-profit organizations, and with governments improves protection not only for our customers but enhances our collective cybersecurity as well.

Partnership on producing cyber threat intelligence is key because no one organization has enough data, analysts or a comprehensive enough understanding of the digital attack surface to ‘go it alone’. While many large companies and government agencies have the resources and talent to maintain in-house threat analysts to do their own research and to customize external sources of data, this is not feasible for smaller organizations. The National Telecommunications and Information Administration’s (NTIA) Communications Supply Chain Risk Information Partnership (C-SCRIP) program created by the Committee for sharing supply chain security risk information with small and rural communications providers and equipment suppliers is a good

[10] www.fortinet.com/fortiguard/labs

example of how government can create and provide relevant and actionable insight on cyber threats to organizations that lack the resources and staff to generate such insight themselves.

Shaping Behavior: Transparency & Trust

With so much of our lives dependent on or enabled by technology, it is important to be able to trust networks and have confidence in the security of the data flowing across them. Accordingly, creating a culture of trust and greater transparency is crucial to enable organizations to make complex cybersecurity decisions, as well as to help users make more informed purchases.

Specifically, consumers need better visibility into key criteria of the IT they use, including where it was developed or manufactured and by whom, and its security posture. We saw this focus on trust at the macro communications network level with the ban on certain companies deemed a national security threat – an effort this Subcommittee was integral in. As digital technology becomes more ubiquitous, we should be asking the same questions about other aspects of our broader communication networks. Is the router in my home secure? Is my television listening to my family dinner conversations? Consumers need to have more trust in the technology they are using in order to build upon the resiliency of our nation's cyber posture. Increased transparency will help to fuel this trust.

Transparency and trust can be addressed through market forces. For example, while the number of IoT devices in use is growing dramatically, many of these devices lack even rudimentary security capabilities and it has even proven difficult for sophisticated consumers to be able to determine which devices have adequate security. The FCC's proposed Cyber Trust Mark program for IOT devices is intended to address this issue in a manner analogous to the Federal Energy Star labeling program that helps consumers evaluate energy efficiency of appliances.[11] Fortinet applauds this initiative and believes that it could serve as a model for enabling more informed decision making in other parts of the cybersecurity marketplace as well.

Government Guidance

The Federal government often creates models and approaches for its own use in addressing hard cyber problems that ultimately gain broader traction and adoption. I helped build the first

[11] https://www.fcc.gov/cybersecurity-certification-mark

version of the NIST Cyber Security Framework that, although intended as a guide and metric for improving cybersecurity within the Federal government, rapidly became a de facto standard for the private sector domestically and internationally. NIST is undertaking a significant revision of this Framework that incorporates feedback and input from these non-Federal users, including Fortinet. In a similar vein, the NTIA's work on generating a "Software Bill of Materials" (SBOM) – a list of the components or ingredients that make up specific software – was a pioneering Federal activity in addressing supply chain risk. A SBOM is analogous to the ingredient label on food packaging, providing transparency and standardization. It ties into activity by NIST and other agencies to track software components and to verify their integrity. Fortinet applauds NTIA's pioneering work in this area, which was drafted with input from multiple stakeholders in an open and transparent process. We believe that this approach should be followed for other hard cyber problems such as AI security that may fall in the remit of NTIA and other agencies.

The power of procurement is another lever Federal agencies can use to shape and influence cybersecurity beyond the US Government. Earlier in this testimony I described the growing intersection between connectivity and security, and the Federal Communications Commission (FCC) E-Rate program that provides funding to assist K-12 schools and libraries in acquiring telecommunications services and technology is an example of this convergence. Adding networking capability without addressing security provides connections that can both compromise users and enable these compromised devices and accounts to be used to attack others. Along with many school districts, Fortinet provided input to the FCC on the need to support the educational community by providing more flexibility for them to access secure solutions. We applaud the Members of this Committee's focus on this critical issue and we strongly support the FCC's efforts to create the Schools and Libraries Cybersecurity Pilot Program for this community.[12] Schools and libraries can use these funds immediately to strengthen their networks and provide a stronger position to fend off future cyber attack. NTIA's Broadband Equity Access and Deployment (BEAD) program is an example of a Federally-funded program where including cybersecurity as an allowable – or even required – element will benefit both the intended users and the nation.

[12] https://docs.fcc.gov/public/attachments/DOC-398397A1.pdf

Conclusion

Throughout my decades of work on cybersecurity in both the public and private sectors I have seen significant improvement in our ability to focus on hard cyber problems and to make progress on solving them even as the underlying technology and the threats we face continue to evolve. Digital services and communications have become more important than ever, and collaboration between government, industry, and individual users is essential for continuing to improve our cybersecurity and cyber resilience. Fortunately, we have a history of innovation and a strong foundation of public-private partnership to build on. Fortinet stands ready to assist the Committee on network security and cybersecurity challenges moving forward. Thank you for the opportunity to be part of this important hearing. I look forward to today's discussion and welcome your questions.