Written Testimony
Amit Yoran
Chairman and CEO, Tenable
House Energy and Commerce Committee
Communications and Technology Subcommittee
“Promoting Security in Wireless Technology”
June 13, 2017

Introduction

Chairman Blackburn, Ranking Member Doyle, and members of the Subcommittee, thank you for the opportunity to testify today on promoting security in wireless technology. The security of mobile devices and wireless networks is a critical aspect in the overall cybersecurity posture of not only the federal government, but also private businesses and consumers everywhere, and I applaud the Committee’s efforts to better understand all aspects of this issue.

My name is Amit Yoran and I am the Chairman and CEO of Tenable. I have spent over 20 years in the cybersecurity field. I received a Master of Science in computer science from the George Washington University and a Bachelor of Science in computer science from the United States Military Academy. I served as the National Cyber Security Director from 2003-2004 and as the founding Director of the 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, acquired by RSA, where I went on to serve as the president of RSA from 2014 through 2016. 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 based in nearby Columbia, Maryland. Tenable has 900 employees globally, more than 23,000 customers worldwide, and more than one million global users. We are the world’s leading provider of vulnerability assessment technology. Our company is focused on transforming security technology through comprehensive solutions that provide continuous visibility and critical context, enabling decisive actions that help our customers protect their respective organizations from growing cyber threats. Our goal is to eliminate blind spots, prioritize threats and reduce exposure and loss.

Simply put, Tenable empowers organizations of all sizes to understand and reduce their cybersecurity risk. This includes the federal government, where Tenable provides the most widely deployed vulnerability management solution.

The Elastic Attack Surface

The modern enterprise environment is dynamic and borderless, with virtually unlimited connectivity. Employees bring personal devices to work, contractors use their computers on corporate networks, and people connect to new cloud instances daily. IT teams spin up virtual machines and services to meet demand, and create and connect microservices-based containers on the fly, decommissioning them just as fast; a process commonly referred to as elastic computing. These mobilization and digitization trends foster a boon in productivity and create agility for the modern enterprise. This is all done while IT teams manage the on-site and legacy architectures, which have been invaded by a slew of enterprise network attached Internet of Things (IoT) devices, including TVs, thermostats, motion sensors, locks, webcams, shades and other control systems to name just a few. According to Business Insider's research service, by 2019 there will be 23.3 billion IoT devices, forty percent (40%) of which will be enterprise IoT devices. These 9.1 billion devices will effectively reside on enterprise wireless networks, representing more than the smartphone and tablet market in their entirety (projected to increase to 6 billion by 2019).[1]

For the first time, concern about IoT security ranked higher in ISACA's State of Cyber Security member survey than concerns about losing mobile devices. Only 13 percent of respondents cited lost mobile devices as an exploitation vector in 2016, compared to 34 percent in 2015. By contrast, 30 percent in 2016 said they were either "extremely" or "very concerned" about IoT in the workplace, with 29 percent saying they were "concerned."[2]

Today's complex mix of computer platforms and environments varies by system longevity, location, manageability, importance and function, yet they combine to represent today's modern attack surface, where the assets themselves and their associated vulnerabilities are constantly expanding, contracting and evolving like a living organism, creating gaps in overall system understanding, security coverage and resulting in exposure.

Nevertheless, mobile device threats still warrant concern. A problem facing many organizations,

[1] Business Insider, "The corporate 'Internet of Things' will encompass more devices than the smartphone and tablet markets combined," http://www.businessinsider.com/the-enterprise-internet-of-things-market-2014-12

[2] ISACA, "State of Cybersecurity 2017," http://www.isaca.org/Knowledge-Center/Research/Documents/state-of-cybersecurity-2017-part-2_res_eng_0517.PDF?regnum=376901

including government, is the workforce using multiple mobile devices – smartphones, tablets, laptops – some of which are owned by the organization, and many of which belong to individuals. To boost productivity, increasingly each of them needs to be able to access organizational networks and resources. This presents several problems, including not knowing who is using which device, whether the devices have the latest software updates, or if device has been tampered with (i.e., jailbroken). Another challenge with mobile devices is their unpredictability: they hop from cellular 3G to 4G to corporate wireless networks seamlessly and are turned off and on at various times.

While still less common than malware targeting desktops, there is an increase in malware specifically designed for mobile devices. Malware attacks against smartphones rose nearly 400 percent in 2016, according to Nokia's 2017 Threat Intelligence Report.[3] Smartphones were the most targeted devices in the second half of the year, the report finds, accounting for 85 percent of all mobile device infections. Security issues pertaining to mobile devices are growing aggressively. Particularly troubling is the rise of nasty "rootkit" malware being distributed to mobile phones via various online stores. This type of malware is quickly rivaling its desktop counterparts in complexity, with sophisticated control of its host, the ability to hide and prevent easy removal.[4]

Vulnerabilities of Wireless Networks

In addition to risks posed by mobile devices, wireless networks present their own set of security challenges. Content traversing wireless networks can frequently be eavesdropped even if it appears to be encrypted. This is a warning that security-conscious consumers should heed.

Organizations frequently add wireless access points (WAPs) to their network to free user laptops and computers from network cables and reduce data charges incurred by cellular carriers. Sometimes organizations have security policies prohibiting wireless access points – but that doesn't mean that others don't add them on their own, a practice referred to as rogue wireless access points.

It's also possible to surreptitiously create a wireless access point on a network. Attackers can configure a WAP so that it appears identical to an organization's actual wireless network. This phenomenon is sometimes known as creating an "evil twin."[5] If an evil twin hits the mark and is

[3] Nokia, "Nokia Threat Intelligence Report 2H 2016," https://pages.nokia.com/8859.Threat.Intelligence.Report.html

[4] International Business Times, "More than 50,000 Android devices may be infected with dangerous 'Dvmap' malware," http://www.ibtimes.co.uk/more-50000-android-devices-may-be-infected-dangerous-dvmap-malware-1625548

[5] SecurityMetrics.com, "Wireless Access Point Protection: Finding Rogue Wi-Fi Networks," http://blog.securitymetrics.com/2016/03/wireless-access-point-protection.html

mistaken for the organization’s wireless network, an authorized user might connect to it, allowing attackers access to the user’s device and where they can steal authentication credentials and access the network seamlessly. Whether it’s an employee or an attacker, or even a piece of malware converting a laptop or other device so that it behaves as a WAP, the effect is that network administrators have lost visibility into the security of that wireless environment, and its impact on the network.

The potential significance of wireless networks is increasing with the addition of IoT devices, which often communicate over wireless. When we talk about the security implications of IoT, we have to think not only about securing the devices themselves, but also the wireless networks on which they operate.

While initial implementation efforts might segregate IoT from enterprise traffic, this is a trend that will likely not be defensible over time, as the desired interaction between people and devices includes the sharing of all kinds of data with each other wirelessly, mandating that sensor, beacons, senders and receivers can seamlessly communicate. Already we have seen sensitive networks hosting industrial control systems connected to enterprise data networks for convenience of administration, where they were formerly segregated onto private "air-gapped" networks.

Methods for creating rogue access points and intercepting traffic holds just as true for cellular networks and the phone conversations and data that they carry. These techniques have been known for years and are readily found. Unidentified signal carriers have been discovered near US military bases.[6] Rogue cellular signals don’t require a massive cell tower or a PhD to create. For $25, you can build one on a cheap, portable and inconspicuous Rasberry Pi.[7]

There are a number of easy to use applications that can provide end to end encryption and protect data and voice communications while using smartphones, such as Wickr, Signal, and TrustCall. These technologies can provide protection, even when communicating over untrusted networks.

There are a number of technologies to help secure mobile devices, such as VMWare’s AirWatch, and other mobile device management (MDM) solutions. Even some cloud-based providers include basic device management and the ability to provide some protection to your data once it’s moved onto a mobile platform. These capabilities frequently include enabling remote wipe, turning on encryption, or setting complex passcodes. There are also technologies that are capable of defining how mobile devices can access your information, who is using them, and if the devices contain vulnerabilities. Mobile security has quickly become a non-negotiable part of any organization’s security program, but it should not be done in isolation.

[6] Popular Science, “Mysterious Phony Cell Towers Could Be Intercepting Your Calls,” http://www.popsci.com/article/technology/mysterious-phony-cell-towers-could-be-intercepting-your-calls

[7] PhoneArena.com, “DIY enthusiasts make their own cell phone tower using a Raspberry Pi,” http://www.phonearena.com/news/DIY-enthusiasts-make-their-own-cell-phone-tower-using-a-Raspberry-Pi_id37976

Solution: Know Your Network

It is critical to recognize that the diversity of the modern compute environment includes on premise servers and computers, wireless, mobile, IoT, cloud, web apps, and containers. And it’s equally important to not take a siloed approach to mobile security or any other aspect of security, but rather view it as part of the holistic ecosystem. As with mobile and the broader ecosystem, the following axiom proves true time and again; you can’t secure what you do not know. If there are elements of your modern computing environment that you don’t have visibility into, chances are they represent misunderstood and unaccounted-for risk.

The highly regarded NIST Cybersecurity Framework validates this. The Framework lays out five essential functions for every cybersecurity effort: identify, protect, detect, respond, and recover. There’s a reason the first function is to “identify”: You can’t successfully implement the other four steps without first knowing what is on your modern compute environment. Likewise, the Continuous Diagnostics and Mitigation (CDM) program, organized by DHS for civilian government agencies, takes a similar approach. According to DHS,

> CDM provides federal departments and agencies with capabilities and tools that identify cybersecurity risks on an ongoing basis, prioritize these risks based upon potential impacts, and enable cybersecurity personnel to mitigate the most significant problems first.

You have to be able to identify assets, so that you can assess risk. You have to know your network and systems – just as an attacker maps out a network before launching an exploit. And knowing your network is more than just the first step in a cybersecurity exercise; it has to be a continuous step, especially as the compute base changes and your attack surface continues to morph indefinitely.

In one example from the PC world, the recent WannaCry and related ransomware attacks could have been prevented if organizations had known their systems, the associated high-profile vulnerabilities and patched them in a timely manner. Continuous visibility into the existence and vulnerability of every asset in the modern computing environment – including mobile devices and wireless networks – is critical to understanding the business impact of any attack. Knowing your network and its vulnerabilities at all times is part of good cyber hygiene, which the Center for Internet Security says consists of five actions: Count, Configure, Control, Patch and Repeat. Again, the first order of business is to count – identify, scan, enumerate, map, or know what is out there. Without that step, the cybersecurity efforts are far less likely to be effective.

Policy Recommendations

I'd also like to offer some policy recommendations that I believe would help secure networks, including wireless, as well as enhance cybersecurity practices.

First, there is a well-documented shortage in the cybersecurity workforce. In order to solve the cybersecurity challenges we face today, we need to make sure we are recruiting, developing and maintaining the best talent. According to the Global Information Security Workforce Study (GISWS) released in February, the workforce shortage is projected to reach 1.8 million people by 2022.[8] Women constitute only 14% of the cybersecurity workforce in North America and just 11% of the cyber workforce globally.

It is up to industry, along with Congress, to increase accountability and reduce this gap. We need a bold, new cyber workforce strategy that develops and advances the ranks of people from all walks of life. While the private sector can lead the way, we need buy-in and partnership from the government.

I know many companies are actively working with the government to address the cybersecurity workforce shortage, but the workforce strategy depends on more than a willingness to change. We must think innovatively and revisit our approach to attracting and retaining talent. Management and leadership courses should be made more inclusive to diversity. Only through increased inclusion and diversity in perspective and thought, can our industry achieve greater creativity, innovation, and develop new solutions to our most vexing challenges. At Tenable, we have implemented a "Rooney Rule" and are setting an example of greater diversity in our leadership ranks.

I do want to state, however, that our efforts to expand the human workforce will inevitably fall short of the insatiable and growing demand for cyber talent, and we have to prepare for that. We need to have a complementary focus on technology and automation so that we can make the most of the human experts we have. Asymmetric leverage of our cyber talent through the use of technology is the only path to success.

Second, the Administration recently released the Cybersecurity Executive Order, which specifically calls out the importance of securing critical infrastructure. The government should encourage private sector companies to continually fully assess their cybersecurity risk, just as federal agencies will be doing and some regulatory requirements and best practices already mandate.

This is an important step forward, and even more still needs to be done. Today all organizations

[8] The Center for Cyber Safety and Education and the Executive Women's Forum on Information Security, Risk Management and Privacy, "The 2017 Global Information Security Workforce Study: Women in Cybersecurity," https://iamcybersafe.org/wp-content/uploads/2017/03/WomensReport.pdf

are part of a global ecosystem and have a cyber hygiene responsibility to one another. This can be thought of using vaccination as an analogy. Simple malware like WannaCry demonstrated what a crippling attack in the future might do. As a result, you had factories closing like Renault in France, hospitals refusing patients such as NHS in the UK, and numerous other examples. While not blaming the victims, the infection was spread company-to-company, many of which simply failed to adequately assess and address their cybersecurity risk.

In some instances patching systems isn't possible or practical. This may be true, but it doesn't alleviate the fundamental responsibility to understand risk and apply appropriate compensating controls or other countermeasures.

In commercial cases this shared responsibility extends to customers and shareholders, and in governments' case, to their citizens. I am not advocating a mandate for some elusive perfect security, but simply stating that good cyber hygiene is in our individual enterprise and global ecosystem's best interest.

Third, in order to see and protect assets, including mobile devices, the federal government should support a modern approach to cybersecurity that is based not only on scanning, but discovery of unknown assets and assessing their vulnerability. With the right technology, agencies can gain real-time visibility into their asset base and where they are exposed, and the insight to help prioritize the risks that matter most. Without such an enlightened and proactive approach, government agencies will never be able to answer the most fundamental questions in security: where and how am I exposed? And what can I do to most efficiently reduce my risk? To reiterate the learnings of the NIST Framework and CDM program, the process starts with a deep knowledge of your systems and their exposures.

Fourth, the federal government can promote the establishment and adoption of best practices by encouraging engagements such as the NIST Cybersecurity Framework. A product of various stakeholders, the Framework has been widely praised and, according to Gartner, will be adopted by 50 percent of organizations by 2020.[9] This public-private initiative is achieving adoption because it's a voluntary, industry-led program that makes sense. It offers a prioritized, flexible, repeatable, and cost-effective approach for enterprise leadership to understand cybersecurity risk. Its recommendations are accessible to cybersecurity professionals and other organizational stakeholders. The federal government should continue to support the NIST Cybersecurity Framework and other efforts to create guidance for improved cybersecurity. One such piece of guidance could be around automated asset discovery for both private and public-sector organizations, fulfilling one of the tenants of the Framework.

[9] Intrinium.com, "NIST Cybersecurity Framework: Adoption or Bust!" https://intrinium.com/nist-cybersecurity-framework-adoption-or-bust/

Finally, it’s worth mentioning the recent legislation relating to IT modernization. It is promising to see Congress rallying behind much-needed measures such as the Modernizing Government Technology Act (MGT Act), sponsored by Representatives Will Hurd and Gerry Connolly. While this legislation involves all systems, not just wireless devices, it represents a meaningful step in the right direction toward providing adequate, risk-based, and cost-effective information technology capabilities that address evolving threats to information security.

Closing

In closing, I want to emphasize the importance of taking an agile, continuous and holistic approach to cybersecurity and technology policy. As we all know, IT is changing quickly along so many dimensions. We should take great care to not consider any aspect of IT in a silo, but rather embed security as an integral part of initiatives where IT assets and connected devices are deployed. Wireless networks are an important part of our technology ecosystem – especially with IoT devices coming online at fantastic rates. Let’s look at wireless networks in the broader context of our agile IT environments, the elastic attack surface and the broader ecosystem of internet technology.

I would like to thank Chairman Blackburn and Ranking Member Doyle and all the members of the Subcommittee for their attention to this important issue. I appreciate the opportunity to be here today and look forward to working with you and your colleagues as cybersecurity topics remain at the forefront of so many policy decisions we face. I will be happy to respond to your questions.