Written Testimony
Hearing of the Pennsylvania House Majority Policy Committee
"Cybersecurity in Pennsylvania"
March 28, 2022, 2:00pm

Chairman Causer and Members of the House Majority Policy Committee, thank you for inviting Palo Alto Networks to submit written testimony for today's hearing on "Cybersecurity in Pennsylvania." The aim of our testimony here is to highlight the major cybersecurity trends we are seeing around the globe and identify opportunities for improving the Commonwealth's cybersecurity ecosystem.

By way of background, Palo Alto Networks is the world's largest cybersecurity provider. Our technologies give over 80,000 enterprise customers the power to protect billions of people worldwide. We employ over 11,000 cybersecurity professionals around the globe and provide security to the most sensitive governmental networks, the Fortune 500, and many of the world's largest critical infrastructure providers. Our mission is simple: "Be the cybersecurity partner of choice, protecting our digital way of life."

Palo Alto Networks has a philosophy of continual innovation designed to meet the changing threat environment and the needs of our customers. We started by pioneering the next generation firewall and have since evolved to provide a comprehensive range of cybersecurity services built around a philosophy of integration and automation. Over the last three years, we have invested over several billion dollars in R&D and acquisitions of key technologies and now have a global intelligence network; best-in-class security for cloud and endpoint; a world-class incident response team; and capabilities that not only allow us to see networks as attackers do, but also can stop those attacks at network speed leveraging machine learning techniques.

Public-private partnerships are a core part of how we enhance global cybersecurity and protect our digital way of life. A critical part of that mission is investing to build the cybersecurity workforce of tomorrow. Starting in 2017, Palo Alto Networks partnered with the Girl Scouts of the USA to launch the first ever national cybersecurity badge program. Since launch, over a quarter million cybersecurity badges have been awarded to girls from kindergarten to 12th Grade across the United States, including in Pennsylvania.

Palo Alto Networks also supports an international Cybersecurity Academy program at over 1,800 institutions globally, aimed at developing the next generation of cybersecurity professionals. Here in Pennsylvania, Palo Alto Networks supports Cybersecurity Academies at Cumberland Perry Area Vocational Technical School (CPAVTS), Millersville University,

Pennsylvania State University, and Saint Vincent College and we are always looking for additional educational institutions with whom we can partner.

Palo Alto Networks has also established a new scholarship program for Historically Black Colleges and Universities (HBCUs). The program includes fourteen $10,000 scholarships for students at HBCUs as well as mentoring and internships opportunities. For students at Cheyney University, Lincoln University, and other HBCU institutions this could be a significant lift.

Emerging Cyber Threats: While there are many different cybersecurity threats, there are four specific types of threats that we want to highlight as areas of particular concern to states and localities: ransomware; industrial control system attacks; supply chain attacks; and exploitation of vulnerabilities.

Ransomware: Ransomware is a profound and growing cybersecurity threat that has gone from a hobby to a lucrative criminal profession and true national security threat. Palo Alto Networks has been tracking ransomware for more than 5 years when average demands were $200-$300. According to a Palo Alto Networks report published on March 24 of this year, in 2021 the average ransom demand was $2.2 million and average ransom paid was $541,000.[1]

One of the most notable ransomware attacks of 2021 was the Colonial Pipeline attack that disrupted oil production and distribution for a system that provided nearly 45 percent of the fuel to the East Coast. While critical infrastructure attacks like Colonial Pipeline make national headlines, healthcare has emerged as one of the most regular targets. Last year, one in five ransomware cases we investigated involved providers that depend on computers to treat patients.[2]

Ransomware gangs operate like high-tech firms, often referring to their victims as "customers." They employ a customer service ticketing system that warns victims when payment deadlines are approaching. They also use slick marketing tools, including a time clock that counts down the hours to deadlines and have "help desks" to facilitate victims pay ransoms.

While there have been improvements within state and local governments, there is much work left to do to prepare for this threat. Palo Alto Networks commissioned and recently released a survey of state and local governments on ransomware preparedness.[3] One of the key findings of the survey was that only 47 percent of respondents currently have an incident response plan for ransomware. The report goes on to read: *"The price for not having an incident response plan is*

---

[1] https://start.paloaltonetworks.com/2022-unit-42-ransomware-threat-report
[2] https://www.paloaltonetworks.com/blog/2021/03/ransomware-threat/#:~:text=Last%20year%2C%20one%20in%20five,malware%20covered%20in%20our%20report.
[3] https://www.paloaltonetworks.com/company/press/2022/while-ransomware-remains-a-top-threat-for-state-and-local-it-leaders--national-survey-shows-response-plans-are-lacking

high. The average cost of a ransomware incident response investigation was $73,851 in 2020, even when backups could be recovered. This number does not include other potential expenses, including ransom paid, downtime and recovery costs, loss of the public's trust and, in worst-case scenarios, loss of life."

At Palo Alto Networks, we have been successful in helping organizations combat ransomware. We work with our customers to conduct Ransomware Readiness Assessments and help ensure that defenses are aligned with best practice standards, like the U.S. National Institute for Standards and Technologies (NIST) *Framework for Ransomware Prevention*. Our goal is to help organizations adopt a multi-pronged, prevention-first strategy that leverages security technologies to drive automation and advanced analytics to prevent ransomware encryption before it occurs.

Industrial Control System Attacks: Industrial control systems (ICS) are the physical systems, like pumps, machine levers and manufacturing systems, that underpin the functions of critical infrastructure facilities like water, electricity, and hospitals. Cyber-enabled ICS attacks can have a kinetic impact in the real world.

An example of such an attack is the Oldsmar Water Treatment Facility breach in Florida in 2021. In this instance, attackers gained access to the systems that controlled the mixture of sodium hydroxide (or lye) in the water supply and were able to make it 100 times higher than normal. Lye poisoning can cause burns, vomiting, severe pain and bleeding. Fortunately, an alert worker at the plant was able to manually stop the attack but it highlights the vulnerability of smaller municipal infrastructure providers.

Successfully defending critical infrastructure requires an approach that foundationally segments key elements within industrial control systems. At Palo Alto Networks, we employ solutions that are Application, User, and Content-aware to help ensure that threats in information technology (IT) systems don't disrupt operational technology (OT) systems. So even if an attacker were able to gain access to a critical infrastructure provider's IT network, they would not be able to affect any critical physical systems as was the case in the Oldsmar attack.

Supply Chain Attacks: A supply chain attack is a cyber attack that seeks to damage an organization by targeting less secure elements in the supply chain. It's a "low and slow" way for attackers to gain access to organizations' networks under the cover of a trusted source, like a software update or remote patch deployment.

One of the most notable recent supply chain attacks was the SolarWinds attack. In this instance, the attackers were able to compromise what should have been a routine software update from a trusted IT provider, SolarWinds. Instead, victim organizations downloaded infected software,

enabling attackers to gain access to sensitive government and corporate networks for hundreds of organizations.

Good technology can effectively identify and stop supply chain attacks by identifying malicious code and anomalous activity. In the case of SolarWinds, Palo Alto Networks Cortex XDR prevented an attempted attack against our own company's network infrastructure by immediately detecting and preventing the infected code from executing the Cobalt Strike Beacon on one of our IT SolarWinds servers. [4]

Vulnerability Exploitation: While many of the cyberattacks described above rely on novel attack methods, attackers will also exploit widely known but unpatched vulnerabilities. Vulnerabilities are weaknesses in software or hardware that may not be known to anyone but the attacker (a 'zero day' vulnerability), or a known vulnerability that an organization hasn't yet patched or mitigated. This can leave an organization's network extremely vulnerable.

One recent, particularly significant vulnerability is known as "Log4shell" and has been commonly cited as one of the most significant vulnerabilities of the last decade. The vulnerability affects Log4j, a piece of open-source software that you've probably never heard of but likely use every day, as its code is embedded in many common applications and cloud services. It was discovered in December 2021 and attackers can use it to take over systems, exfiltrate data, and do other damage.

What makes Log4shell so significant is the ubiquitous nature of the software in large widely used systems including Amazon, Microsoft, Minecraft, and more. Palo Alto Networks was recently appointed to the newly established Cyber Safety Review Board– a body modeled after the National Transportation Safety Board that assesses transportation crashes– to make recommendations about how to improve the national response to cyber incidents like the Log4shell vulnerability.

Unmitigated vulnerabilities pose such a serious threat that the U.S. Cybersecurity and Infrastructure Security Agency (CISA) has established a "Known Exploited Vulnerability" catalog that currently lists over 500 known vulnerabilities. While many of these vulnerabilities are not necessarily new, the known exploitation of these vulnerabilities prompted CISA to undertake this national campaign to encourage better patching and management across the cybersecurity ecosystem.

[4] https://www.paloaltonetworks.com/blog/2020/12/solarwinds-statement-solarstorm/

Organizations that attain better visibility of their internet-facing "attack surface" can more rapidly identify and remediate vulnerabilities. Having this attacker view of your network's weaknesses is foundational to implementing sound cybersecurity strategies and policies. Palo Alto Networks has a proprietary tool called Cortex Xpanse that can look across the full range of an organization's internet-facing architecture to put together a potential attacker's view of an organization's threat surface. This type of insight into vulnerabilities is foundational to mitigating and reducing overall cybersecurity risk.

New Threat Environment Requires New Cybersecurity Approaches: By all accounts, the COVID-19 pandemic has changed how and where we work, now and into the future. It exponentially increased companies and governments' migration to the cloud and changed the boundaries between work and home, most likely forever.

Working remotely requires a different security solution set, especially as data moves back and forth between the public cloud and an organization's internal networks. This new paradigm makes a Zero Trust approach to cybersecurity so critical. Zero Trust is a cybersecurity strategy premised on the idea that no user or asset is to be implicitly trusted. It assumes that a breach has already occurred or will occur, and therefore, a user should not be granted access to sensitive information by a single verification. Instead, each user, device, application, and transaction must be continually verified to be able to access an organization's sensitive computing resources. This is especially important in a remote work environment where traditional network boundaries have all but disappeared.

To address this evolving threat landscape, our aim at Palo Alto Networks is to help customers attain three core capabilities. The first is comprehensive visibility of their networks. The mantra "you can't protect what you can't see" is foundational to sound cybersecurity.

The second capability is relentless automation. One of the biggest challenges facing state and local governments is a significant workforce shortage of qualified cybersecurity professionals. By automating cybersecurity wherever and whenever possible, state and local governments can maximize their scarce workforce resources to only high order, sophisticated tasks worthy of human intervention.

Relatedly, the third capability is actionable security. Security alerts need to provide a path to proactive prevention and remediation. The more actionable and specific the alerts are, the more efficient and effective cybersecurity professionals can be to stop the different types of common cyber attacks described above.

A Unique Cybersecurity Investment Opportunity. Last year's passage of the Bipartisan Infrastructure Framework created the first ever State and Local cybersecurity grant program, which includes over $1 billion in grants to improve cybersecurity capabilities. While these

grants will not be enough to fund all the cybersecurity needs of these entities, they do provide a unique opportunity for states to invest to improve their overall cybersecurity ecosystem.

These grants can serve as a forcing function for state and local governments to work together in new ways to develop multi-entity approaches to cybersecurity at the state, city, county, and municipal levels. We have seen several states taking significant steps in this direction including North Dakota, New York, Massachusetts, Louisiana, and others. Pennsylvania has a similar opportunity to leverage these grants and the planning processes involved to develop a cybersecurity ecosystem that can better defend the entire Commonwealth.

Thank you for the opportunity to provide Palo Alto Networks perspective on how – through close public-private partnership – we can collaborate to mitigate the serious cybersecurity risks that face Pennsylvanians, the nation, and the entire world. We stand ready to continue to be a resource to this Committee, the bipartisan House Cybersecurity Caucus, and the entire Pennsylvania State Legislature to advance this important dialogue.