Written Testimony of:

Sam Kaplan
Senior Director and Assistant General Counsel, Public Policy & Government Affairs

Palo Alto Networks

Before the:

Senate Committee on Commerce, Science, and Transportation
Subcommittee on Consumer Protection, Product Safety, and Data Security

Regarding:

Strengthening Data Security to Protect Consumers

May 8, 2024
2:30 PM EDT

Chairman Hickenlooper, Ranking Member Blackburn, and distinguished members of the committee:

Thank you for the opportunity to testify on the importance of data security. Your committee's interest in better understanding cybersecurity's foundational role in enabling data privacy is greatly appreciated. My name is Sam Kaplan, and I am the Senior Director and Assistant General Counsel, Public Policy & Government Affairs at Palo Alto Networks. I've spent the bulk of my career working at the intersection of cybersecurity, national security, and data privacy. On behalf of my company, I offer our commitment to work in partnership with you and your staffs as you continue to examine this important area of public policy.

For those not familiar with Palo Alto Networks, we were founded in 2005 and have since become the global cybersecurity leader – protecting businesses, people, and governments across more than 150 countries. We support 95 of the Fortune 100, critical infrastructure operators of all shapes and sizes, the U.S. federal government, universities, educational institutions, and a wide range of state and local partners.

Practically speaking, this means we have a unique vantage point into the cyber threat landscape. This information, paired with the insights we develop from helping organizations respond on a daily basis to complex cybersecurity incidents, puts us on the front lines of the cyber defense battle. We are committed to using this mantle to be good cyber citizens and trusted security partners.

Cybersecurity Enables Data Privacy

Palo Alto Networks strongly believes that deploying cutting-edge cybersecurity defenses is a necessary enabler of data privacy. Organizations should be encouraged to protect data by implementing robust data and network security practices that both can help prevent cyber incidents and data breaches from occurring in the first place, and mitigate the impact should an incident occur.

Palo Alto Networks supports efforts to develop a strong federal privacy standard that:

1. Provides consistent and predictable requirements and protections for individuals and businesses;
2. Establishes a single national standard to prevent a complex compliance patchwork;
3. Promotes robust and adaptable data security standards, spanning prevention to response, commensurate with today's evolving cyber threat environment;
4. Fosters innovation by recognizing the importance of automation in data security;
5. Prevents disclosure and transparency requirements from unintentionally creating roadmaps for threat actors to break through data and network defenses; and
6. Recognizes the beneficial uses of security data for permitted purposes, such as cybersecurity.

To keep pace with and respond to the increasingly sophisticated threat landscape, the cybersecurity community regularly leverages security data, through which cyber threat information is synthesized to develop a holistic picture of the techniques, tactics, infrastructure, and motives of cyber adversaries. Security data is the network telemetry – the 1s and 0s, the malware analysis, the IP addresses, the vulnerability enumeration – that we ingest and analyze to help defenders stay ahead of attackers.

The necessity of cybersecurity firms collecting, processing, retaining, and transferring security data cannot be stressed enough. As explained further below, automated cyber defense tools are already proving transformational for network defenders. Security data – across the network, endpoint, and cloud – is now enhanced, stitched together, and correlated in real-time to differentiate the threat signal from the noise. This, in turn, results in better fortified systems and enhanced data security.

To that end, recent policy approaches recognizing the importance of leveraging security data to bolster cyber defense is a positive development and one that will meaningfully help protect data privacy. Palo Alto Networks appreciates the growing recognition of this critical point, and believes that data privacy legislation should ensure that access to information for cyber defense purposes is not undermined by requirements intended to address other uses of consumer data.

Any federal privacy law must ensure that cyber defenders can leverage security data to prevent, detect, protect against, and respond to both known and unknown security vulnerabilities – bolstering both privacy and national security imperatives.

Today's Threat Landscape Demands Enhanced Data Security

With the growing volume and sophistication of today's threats, it is critical for organizations to understand the threat landscape and how to properly defend against it. Every member of this committee likely has had a business, bank, school, or local government entity in their state victimized by a cybersecurity attack or data breach. These attacks affect our daily lives – from disruptions of public services like healthcare or emergency services, to leakage of Americans' sensitive data.

Data breaches can result from several factors, including weak credentials, misconfigured security settings, internet-facing software vulnerabilities, and phishing attacks. These incidents can involve significant financial loss and damage to an organization's reputation, and compromise the security of individuals' critical data.

This threat is not subsiding. Instead, adversaries continue to enhance their techniques and increase their sophistication. Bad actors can now execute numerous attacks simultaneously against one company, leveraging multiple vulnerabilities at once. We are also seeing evidence that adversaries are using AI to enhance what we call social engineering attacks – phishing emails and voice calls designed to lure users to "click the link" or provide access.

A sobering yet persistent reality of our connected world is that far too many “digital doors” are left open for adversaries to walk through with relative ease.

It is often said the internet looks very small to an attacker but massive to a defender. After all, an enterprise that closes 99% of its digital doors but leaves one open inadvertently may well be destined for a breach. Entities of all sizes, public and private, have historically struggled to understand and manage their digital infrastructure, including phones, laptops, servers, and applications that have been exposed to the internet. In fact, we have found that even sophisticated enterprises actually have twice the number of systems exposed on the internet than what they were internally monitoring – a visibility gap that gives adversaries the upper hand.

The threat intelligence and incident response division at Palo Alto Networks, known as Unit 42, helps assess and test the security controls of organizations, transform their security strategies with a threat-informed approach, and respond to incidents in record time. In 45% of incident response cases led by Unit 42 last year, attackers exfiltrated data in less than a day after compromise, down from 44 days as recently as 2021. Slow response times increase the cost of resolving incidents, and increase the likelihood of sensitive data being compromised.

Complementing our insights from incident response cases, Palo Alto Networks also leverages a capability that indexes the public-facing internet through the eyes of the adversary to discover exposed systems, vulnerabilities, and misconfigurations. We are increasingly seeing cloud infrastructure as an inviting attack vector for adversaries. In fact, over 80% of the exposures we observed were cloud-based, and Unit 42 similarly saw a 115% increase in cloud-related incidents in 2023 compared to 2022.

Modern organizations often depend on multiple cloud environments to store, process, and analyze data. The use of diverse cloud services drives many helpful operational efficiencies, but also creates fragmentation – scattering sensitive records across multiple datastores with opaque data flows, and complicated access control mechanisms. Organizations frequently struggle to understand what sensitive data (e.g., customer details, health data, financial information) they actually hold, who can access it, and where it is at risk.

Recognizing these realities, promoting effective data security requires an innovative approach to fortifying cyber defenses, particularly given the constantly evolving threat landscape.

Securing Systems and Data with AI and Automation

Fortunately, AI and automation are proving transformative for network defenders, enabling organizations not only to respond more quickly, but also to more nimbly ingest and analyze security data to proactively harden their networks against attacks.

One of the most promising applications of AI and automation for cyber defense is to significantly uplevel and enhance the capabilities within Security Operation Centers (SOCs). For too long, our community's most precious cyber resources – people – have been inundated with security alerts that require manual triage, forcing them to play an inefficient game of "whack-a-mole," while vulnerabilities remain exposed and critical alerts are missed.

Two of the most important metrics for any security operations team are Mean Time to Detect and Mean Time to Respond. As the terms suggest, these metrics provide quantifiable data points for network defenders about how quickly they discover potential security incidents and then how quickly they can contain them to help mitigate their potential impact.

Historically, organizations have struggled to execute against these metrics. A recent Unit 42 report that analyzed real-world cloud-related incident response cases found that, on average, security teams take nearly six days to resolve an alert. In contrast, we now see many adversaries moving from compromise to data exfiltration in just hours.

Giving defenders the upper hand requires a new approach that leverages AI-driven SOCs. This technology will be a force multiplier for our cybersecurity professionals and will substantially reduce incident detection and response times.

Early results from deploying this technology on our own company networks have been particularly promising. On average, we ingest 36 billion events daily and use AI-driven data analysis to automatically triage that number down to just eight that require manual analysis. In addition, we have reduced our Mean Time to Detect to just 10 seconds and our Mean Time to Respond to just one minute for high priority alerts.

Early customer benefits have been similarly encouraging. We have already seen a reduction in mean response times from weeks and days to hours and minutes. Such a reduction is critical to stopping threat actors before they can encrypt systems or steal sensitive information, and for minimizing the impact of an incident. This tool has dramatically improved incident close-out rates from 20% pre-deployment to 100% post-deployment.

Increased adversarial speed to steal or encrypt data demands rapid detection and response. In order to stay a step ahead of sophisticated adversaries, we must also detect never-before-seen anomalous behavior, not just previously identified attack patterns. AI now gives us the capability to do so – putting network defenders back in the driver's seat, not a step behind.

Key Data Security Recommendations

As organizations seek to enhance their cybersecurity and data security postures, Palo Alto networks offers the following recommendations:

1. Ensure complete visibility of attack surfaces: 75% of attacks and breaches fielded by Unit 42's incident response team result from a common culprit – internet-facing attack surface exposures. Deploying solutions that provide centralized, near real-time visibility can help organizations identify and mitigate vulnerabilities before they can be exploited.

2. Promote Secure AI by Design: Enterprises will benefit from capabilities that assist in inventorying AI usage, applying policy controls, and securing apps built with AI.
3. Leverage the power of AI and automation in network defense to modernize security operations and reduce the burden on overworked analysts. The latest technology can help organizations drive down key cybersecurity metrics like Mean Time to Detect and Mean Time to Respond, denying attackers the time they need to compromise an organization's systems or exfiltrate its data. Additionally, technique-based protections mapped to the MITRE ATT&CK Framework can help defenses nimbly evolve in response to adversarial tactics.
4. Implement enterprise-wide zero trust network architecture: This is a fundamental security principle that assumes the network is already compromised and implements processes that continuously validate the user, device, application, and data in a controlled manner. Zero trust network architecture creates layers of security that prevent or limit an attacker from successfully moving laterally around the network. This provides victims with more time to detect, properly contain, and remediate the threat.
5. Protect cloud infrastructure, applications, and data: With cloud migration accelerating, threat actors will continue to develop tactics, techniques, and procedures designed to target and compromise cloud workloads. Organizations leveraging cloud infrastructure should implement a cloud security program and platform that offers comprehensive cloud-native application protection.
6. Maintain an incident response plan to prepare for and respond to cyber incidents, including emerging ransomware tactics like extortion, multi-extortion, and harassment. Organizations that continuously review, update, and test their incident response plans – ideally with input from cybersecurity experts – are much more likely to effectively respond to and contain an active attack. Organizational leadership must elevate cybersecurity as a core part of their overall enterprise risk management strategy.

While there is no silver bullet in cybersecurity, prioritizing these recommendations will materially reduce the risk of falling victim to an attack, more effectively protect data if an attack does occur, and help increase the resilience of the entire cybersecurity ecosystem.

Partnerships and People Remain Critical

It is often said that cybersecurity is a team sport, and partnership is very much in our DNA at Palo Alto Networks – and across the entire cybersecurity industry.

Palo Alto Networks is proud to be a founding Alliance member of CISA's Joint Cyber Defense Collaborative (JCDC). In forums like these, we share technical threat intelligence on a daily basis through partnerships with U.S. government entities, private sector entities, and other allied nations to support global prevention and response to significant cyber incidents. We are also active members of the NIST National Cybersecurity Center of Excellence projects on 5G, zero trust, and post-quantum cryptography.

It is critical we educate and train the cyber workforce of today and tomorrow with the advanced skills required for meaningful jobs that complement technological innovation. This approach is fundamental to improving our collective cyber defense and enabling data security.

To that end, we have been encouraged to see the impact of several initiatives aimed at broadening access to cybersecurity education, including the Palo Alto Networks Cybersecurity Academy, which offers free and accessible curricula aligned to the NIST National Initiative for Cybersecurity Education (NICE) Framework, to academic institutions from middle school through college. Hands-on experiences with cyber and AI benefit the entire ecosystem as they help to upskill our own workforce as well as that of our customers.

Palo Alto Networks offers several accelerated onboarding programs to diversify the workforce, including the *Unit 42 Academy*, which welcomes new early career participants each August as full-time members of our incident response and cyber risk management teams. We are pleased to report that our 2023-2024 class is 80% female.

Taken together, the aspects I've highlighted in my testimony will help address a number of components associated with a holistic approach to data security – technology, processes, and people.

Thank you for the opportunity to testify. I look forward to your questions.