Regulatory Oversight Podcast: Decoding Cyber Threats: Protecting Critical Infrastructure in a Digital World

Hosts: Stephen Piepgrass, Gene Fishel, and Judy Jagdmann
Guest: Sam Kaplan

Stephen Piepgrass:

Welcome to another episode *of Regulatory Oversight*, a podcast that focuses on providing expert perspective on trends that drive regulatory enforcement activity.

I'm Stephen Piepgrass, one of the hosts of the podcast and the leader of the firm's Regulatory Investigations Strategy and Enforcement Practice Group. This podcast features insights from members of our practice group, including its nationally ranked State Attorneys General practice, as well as guest commentary from business leaders, regulatory experts, and current and former government officials. We cover a wide range of topics affecting businesses operating in highly regulated areas.

Before we get started today, I want to remind all our listeners to visit and subscribe to our blog at regulatoryoversight.com so you can stay up to date on developments and changes in the regulatory landscape.

Today, two of my colleagues, Gene Fishel and Judy Jagdmann, speak with Sam Kaplan of Palo Alto Networks on the issues of cyber threats facing critical infrastructure companies, the government's response to cyber incidents, and using AI to potentially combat cybersecurity threats. Sam is the Director and Senior Global Policy Counsel for Palo Alto Networks.

He's responsible for providing legal advice on a diverse range of domestic and international policy initiatives, with a particular focus on global cybersecurity law, critical infrastructure protection, privacy and data security, and public private capacity building. Prior to transitioning to the private sector, Sam served as the Assistant Secretary for Cyber, Infrastructure, Risk, and Resilience Policy at the U.S. Department of Homeland Security, where he led DHS policy development in support of department wide efforts to reduce national risks, with a focus on critical infrastructure, cybersecurity, federal network security, countering cybercrime, and improving the security and resilience of the global cyber ecosystem.

Can't think of a better expert to address these topics with us today. And I know we're all looking forward to this discussion.

Judy Jagdmann:

Thank you, Steven, for your introduction of Gene, and me, and for introducing this podcast. Gene and I are both veterans of the Office of the Attorney General for Virginia. Gene was the Senior Assistant Attorney General and Chief of the Computer Crime Section. I was the deputy in charge of the multi-state unit for many years. We're both very familiar with multi-state actions, and we're both familiar with the importance of cybersecurity. Gene, in particular, his whole career has focused on these issues.

Regulatory Oversight Podcast: Decoding Cyber Threats: Protecting Critical Infrastructure in a Digital World

After I left the Attorney General's office, I was on our Public Service Commission, and the last at least, seven to 10 years, cybersecurity has been a very hot issue, as our utilities are considered critical infrastructure, and subject to heightened needs for security. Our guest speaker today is Sam Kaplan, he is the Assistant General Counsel for Public Policy and Government Affairs for Palo Alto Networks. Thanks for being with us today, Sam.

Sam Kaplan:

Perfect. Thank you for that introduction, Judy, and thanks to everybody for inviting me to be a part of this podcast. I'll always jump at the chance to talk about cybersecurity and critical infrastructure protection, so it's a pleasure to be here.

Judy Jagdmann:

Well, thank you again. First, would you describe what Palo Alto Networks does, and a little bit about your job, and the scope of the cyber threat we're now facing?

Sam Kaplan:

Sure, I'm more than happy to. Just at the outset, I know we're going to have a wide-ranging conversation here today. I do want to note, especially when we get into some of the regulatory discussion that some of the opinions are those opinions of myself and do not represent the position of Palo Alto Networks. But again, happy to be here. Top level, Palo Alto Networks is the world's largest pure play cybersecurity company. A good way to think of our mission is really simply that we are a cybersecurity partner of choice, and our mission is to protect our digital way of life.

Size-wise, we have approximately 13,500 employees located both in the United States and across the globe. We protect and provide cybersecurity services to many of the world's most sensitive networks and systems, both here in the United States, but also abroad. This includes 10 of the Fortune 10 largest companies, eight of the largest banks, nine of the largest manufacturing companies in the world, nine of the 10 largest utilities in the world, seven of the 10 largest oil and gas companies, and nine out of the 10 top hospitals in the US.

We have a full stack cybersecurity service enterprise. We started in 2005, providing hardware firewalls. As our technology grew, that started to evolve into virtual firewalls. Then, really beginning in about 2016, our slate of cybersecurity services really began to expand, and we now offer a full stack cybersecurity solution both in individualized products and services. But that includes our traditional firewall business. But now, we have branched out into attack surface management capabilities, real time SOC automation capabilities. We have a full suite and specific unit dedicated to cyber threat intelligence. They also provide cyber counseling services, incident response services. We really do have sort of a full suite of cybersecurity products.

My role at Palo Alto Networks, sort of a good way to think about my role is, I'm the Lead Global Policy Counsel for Palo Alto Networks. I work with our public policy teams in our legal department, and I provide legal advice and guidance on regulations, consultations, rulemakings, legislation that is occurring both in the United States and abroad. Substance-wise, the big buckets that I deal with are naturally cybersecurity law and regulation. I do a big bucket of work in data flows, and privacy, and also, lately, especially over the past year, have been dedicating

a lot of my time to AI regulation, both in the United States and abroad. That's just a quick top level of me and our company.

Judy Jagdmann:

Thank you, Sam. Could you give us your view of the cyber threat today?

Sam Kaplan:

Sure. I'll sort of couch my view of the cyber threat today, really, in terms of what we're seeing across the globe. Earlier, I've referenced our cyber threat intelligence unit, it's called Unit 42. They have global visibility both across our customer sets, given the nature of our business. But just to put this in context for everybody, through Unit 42, and our cybersecurity products, every day, we analyze 750 million new and unique security objects. These are threats, vulnerabilities, notices, alerts that cross our transom.

Additionally, every day, we detect 1.5 million unique attacks weren't there the day before. This is all due to the efficacy of our tools, and capabilities, and our cyber threat analysts. A lot of those being AI driven. As a result, we have developed this process of continuous discovery and analysis that allows our threat detection tools to stay ahead of that adversary. And that real time awareness of that threat landscape allows our company the ability to block 8.6 billion attacks that are occurring every single day across our networks.

As a result, and from some of our analysis that's put together through our Unit 42, I bucket the cyber threat landscape into really four principal buckets is what we're seeing with regard to trends. Ransomware, industrial control system attacks, vulnerability exploitation, and supply chain attacks. With respect to ransomware, Unit 42 actually releases an annual report on what they're seeing with respect to ransomware trends. Last year's report in 2023, our Unit 42 has really seen those ransomware demands really hit, and the ranges of ransom that these organizations are looking for have range between $3,000 and can go as high as 50 million US dollars.

Over that time, and over the last year, the medium ransomware demand we've seen extorted from victim companies has been around $650,000. For those organizations that did make a ransomware payment, that medium ransomware payment that was tendered from these victim organizations was around $350,000. With respect to notable ransomware attacks, I think the most notable one, and I'm sure we'll talk about this one later was the 2021 Colonial Pipeline attack, that disrupted oil production across the East Coast from the Southeast, up and down the East Coast. Colonial Pipeline particularly provides nearly 45% of the fuel to the East Coast.

In this particular attack, ransomware actors gained access through compromised VPN credentials, or those are the credentials that a lot of us through our companies are using to securely connect to those networks and systems. Once they were able to penetrate through that vector, they exfiltrated around 100 gigabytes of data before they actually encrypted some of those businesses systems. As a result of that encryption, the company took proactive steps and they shut down just over 5,000 miles of pipeline as a precautionary measure so as not to have collateral consequences across their networks and systems.

The company ended up paying $4.4 million in ransom in that particular attack. They paid it in Bitcoin. Through working with the Department of Justice, their cyber task force, they were able to recover that Bitcoin. But because of the fluctuation in price, that recovery was about $2.3 million. What we've seen most interesting with regard to these ransomware groups and these ransomware attacks is our Unit 42, and this is all included in our report. They've seen these ransomware gangs, and they're really starting to operate like high-tech firms. This is through leaked emails that are available on the open and public internet through other reporting. But some of these gangs have started referring to their victims as customers.

They employ customer service tickets to address and warm victims when payment deadlines are approaching. They also have slick marketing materials that they've been able to employ that include a time clock that counts down the hours to a deadline, and they have helped desks that help some of these victim organizations facilitate on how to make the payment to these organizations. We've really seen an uptick in these ransomware attacks on state and local governments.

Palo Alto Networks recently commissioned and released a report, this was last year, on ransomware preparedness across state and local governments. One of the key findings of that survey was that 47% of those respondents, and the state and local level. Only 47% had an incident response plan to deal with ransomware. That report goes on to say that price of not having an incident response plan is deceptively high. The average cost of a ransomware incident to a state and local government was right around $73,000 in 2020. Even where the backups were able to be recovered for those organizations where they could restore the operation of their systems. Importantly, that number, and that cost doesn't include other potential expenses. That includes the ransomware, the downtime, and the recovery cost of those systems, and the loss of the public trust.

The second major bucket that I talked about was these industrial control systems attacks. For critical infrastructure operators in particular, industrial control systems, I think of those as the physical systems like the gears that really underpinned the function of the critical infrastructure facilities like water, electricity, or even hospitals. For this bucket of attacks, these ICS attacks, importantly, they not only can have an impact on the networks and systems themselves, these can have a kinetic impact in the real world. If there is a corruption of a system that's running a power, or a water pumping service, that technological attack can disrupt in the physical world.

We have seen within the last year, there was a state-sponsored attack out of China. This was publicly reported through the Federal Bureau of Investigation, and threat advisories that they put out called Volt Typhoon. In that particular case, the threat actor sought to blend normal networking activity to routine traffic that would compromise those small computers. Additionally, we've seen the federal government send out additional alerts against critical infrastructure with regard to these critical infrastructure and ICS attacks in particular. Again, just because of the kinetic impact that they can have in the real world.

That third bucket, the exploitation of known and unknown vulnerabilities, these are legacy systems, networks that have not been updated to the latest software operating systems. Threat actors are well aware of the libraries of these known exploited vulnerabilities. They're consistently and constantly probing organizations to see where these patches haven't been applied. Again, this is widespread, we've seen this particularly in critical infrastructures, a lot of

those legacy systems just need to be updated to the latest software tools or development. Those known exploited vulnerabilities are critical to address.

CISA, the Cybersecurity and Infrastructure Security Agency actually publishes a list that is constantly updated of known exploited vulnerabilities that they've seen across federal networks, but also across critical infrastructure sectors. That last bucket is a supply chain attack. A supply chain attack is one that seeks to damage an organization by testing and targeting the less secure elements in that technology supply chain. We tend to think of this as a low and slow way for the attackers to gain access to those organizations and networks under the cover of a trusted source. One of the more prevalent attacks that we've seen in this came through a software update. The threat actors were able to embed malware within a software update that was pushed through a company's normal update or update cadence to victim systems. That malware was then able to propagate across those victim systems. It came from that trusted source, the normal software update. But that malicious software really is what started to perpetrate. Those are the four buckets that we've seen, particularly across governments, and the critical infrastructure sector.

Judy Jagdmann:

I'm going to turn it over to Gene now for a few questions. But before I go, what I'm hearing you say is, everyone has to be hypervigilant all the time. This is an ever changing and evolving problem that requires our constant attention.

Sam Kaplan:

Constant battle, correct.

Gene Fishel:

Thank you, Judy, and thank you, Sam. Certainly, before I go on, I have to mention that Judy actually served as the Attorney General of Virginia. She was being modest, and didn't mention that, but she brings a wealth of experience from the regulatory side. Thank you again, Sam, for joining us. I know, during my time. 20 years as a prosecutor, a cybercrime prosecutor, I saw the rise of ransomware incidents. It really has become a form of organized crime, as certainly the more sophisticated operations as you alluded to.

I think the protection of our critical infrastructure needs to be a top priority, as we saw with colonial pipelines. But I want to ask you, based on your experience, and what Palo Alto is seeing. I know Palo Alto is one of the leaders in cybersecurity and compliance. What are you all seeing as the current state of the cyber protection of critical infrastructure? Are we doing enough to protect our critical systems?

Sam Kaplan:

That's a really great point. As both Judy and you said, this is a constant battle. The threat is constantly evolving and metastasizing to newer particular forms. Given that evolving threat landscape, it's ever more important for organizations to stay vigilant, and continue to stay dialed in to sort of how cyber threats are beginning to develop. When it comes specific to critical infrastructure, one of the things that we've seen from the Unit 42 perspective is first and

foremost, across critical infrastructures. Principally, because across the US, there is a very – it's not fragmented, but it is a multi-layered sort of structure of critical infrastructure operators.

Some provides entire state, some are very localized. To me, and again, this is one person's opinion. That sort of different structure. and the ability to layer capabilities on capabilities actually promote some of the resilience in critical infrastructure to withstand attacks in some of these areas. There's a little bit of redundancy by design in there. but that doesn't sort of mitigate. There are areas where critical infrastructure operators will be providing services, and they're the lone game in town. Yes, these are all serious issues on the cyber side.

One of the things that we've seen particularly to critical infrastructure are legacy systems. Critical infrastructure, they often use legacy systems that are far beyond a reasonable lifespan from a security standpoint. This means that many systems are running older, unsupported operating systems. Sometimes, you get so far down in the versioning history of a particular software, they oftentimes cannot be easily patched or upgraded. Additionally, some of those operating systems, those ICS systems that I was referring to earlier, you have to update collateral software across those systems. When you start updating that software, and looking at the chaining out there, it's not an easy thing to update some of these systems because there can be an operational, or a compliance issue. or warranty issues with some of these systems.

Additionally, what we've seen in critical infrastructure is IT/OT convergence. What this is, is more and more of that operational technology, those ICS systems are increasingly relying on IT systems, or networks to sort of operationalize and function. What this has done is that many of those OT systems, those operational technology systems that were previously isolated are now accessible through networks and connections. They are now open to these new cyber vulnerabilities, and it makes them more available, and more at risk of being attacked.

A third sort of bucket that we've seen is across critical infrastructure. I think, a number of additional countries, but particularly with critical infrastructure is a real lack of skilled resources. Critical infrastructure operators, they don't have the full slate of dedicated security personnel with the cybersecurity skills needed to sort of protect those networks. We've seen a need across the cybersecurity industry for cybersecurity professionals to get into this field. I think even the White House Office of the National Cyber Director published a report on the cyber workforce last year. That was estimating, I think the number was around 850,000 jobs and personnel that are needed in this space just to meet with current demands. When you start talking about this expanding threat landscape, and more, and more capabilities going online, that sort of delta between the resources and the personnel available, and the actual need is only going to continue to grow.

One of the unique things that we've seen in the critical infrastructure space too, is sort of regulatory compliance. There are rules and regulations across many critical infrastructure verticals that can create complexity with how these operators can interact with their systems, and how they need to make them available. The last is data. I think, for critical infrastructure with some of these systems, knowing the amount of data that their network infrastructure is developing, and how to make use of that data to detect vulnerabilities attacks, and having the ability to really make use of that data is just a continual challenge that we've seen across critical infrastructure sectors.

Gene Fishel:

I think that certainly highlights the difficulty and marshalling both money and expertise in this area. I think, certainly, funding needs to be allocated to improve the protection of our critical infrastructure. Your last point really leads to our next topic, and I'm going to actually turn it over to Judy to cover this next topic here.

Judy Jagdmann:

Sam, thank you, and thank you, Gene. Sam, you touched on this. This is basically, I guess, just to underscore a little bit. I wanted to hear your views on cybersecurity. I guess the scope of regulation of cybersecurity. In some areas, it seems to be multi-tiered and the requirements are coming from several different departments of government. The bulk electric system comes to mind. You have more than one division of Homeland Security, have rules and requirements. You have the Federal Energy Regulatory Commission enforces rules from NERC, which is the agency that was set up specifically for security of the bulk electric system.

Now, recently, we had the Securities and Exchange Commission issued a set of cyber security rules that it applies more globally, but it also applies to the bulk electric system. In this area, you can have not necessarily competing, but in some instances, overlapping and complicating the reporting requirements. In other areas, there really just isn't that much. We saw recently, with, I guess the EPA's water rule. They withdrew that rule, that regulation wasn't a good fit under the statute they were using, and that Congress is going to enact legislation, and provide money, and resources. Which is probably more appropriate, given the fact that some of these water systems are very small, and they really need help comply. But anyway, what is your thought on the overlapping nature? Any thoughts on improvement that can happen in that area?

Sam Kaplan:

Sure. As you referenced, one of the things that I've done, and I've worked in this space for a long time, I was actually with the federal government before transitioning to the private sector. I was at the Department of Homeland Security for a long period of time, working on cybersecurity and infrastructure protection there. For organizations, understanding the regulatory landscape, I think one of the best first tools is to sort of baseline your understanding. You got to figure out sort of who's who in the zoo, depending on what your organization is. It really takes companies, critical infrastructure providers, or folks working in other sectors, knowing what their sector is, having the ability to sort of determine how that regulation has been structured across the federal government.

If you look at cybersecurity regulation, to me, this goes back to post Homeland Security Act legislation. Where that was what really enabled the federal government to sort of develop its architecture and framework for the 16 critical infrastructure sectors. That's been operationalized through PPD 21, which we understand it's in the process of being updated by the White House, and they might be adding sectors to that. For the cyber side, that sort of 16 critical infrastructure sector has tiered down, because for certain sectors, there are sector specific agencies like the Department of Energy, the Department of Health and Human Services. They're the ones that really have the regulatory prerogative to oversee what those critical infrastructure sectors are doing. They're the ones formulating.

You brought up some of the electric on bulk power, some of those regulations. But that sort of 16 critical infrastructure sector is really foundational. For those companies, you have to understand, what agencies you're dealing with. For example, the Department of Homeland Security of the 16 sectors, DHS has nine of those sectors that they are the sector specific agency for. On top of that, CISA is really supposed to be the central point of coordination for how those sectors specific agencies develop and operationalize their regulatory approach. It's complex, it's multifaceted. There are overlapping rules. You brought up the SEC rule for critical infrastructure, coming out of the NDAA. Two years ago now, there's that CIRCIA bill, which is the Cyber Incident Reporting for Critical Infrastructure Act. That was included as a part of the NDAA. That's putting cyber incident requirements on all critical infrastructure sectors across the 16th.

As soon as they spot an incident, within 72 hours of that discovery of that incident, they have to do an impact assessment. They have to report to CISA. CISA is going to become sort of a central clearinghouse for a lot of that cyber incident. CISA's currently in the rulemaking process for that now. They released a request for information last year. We are expecting them to release language on a rule sometime within this calendar year, I would expect. Because under the NDAA, they had 42 months, I believe it was, to finalize a role in that sector. You tear that, the CIRCIA requirements against the SEC requirements, where critical infrastructure operators are also publicly traded. You have to cyber incident reporting requirements just in that area.

To add the complexity on top of that, the Federal Acquisitions Council just issued a regulation in December for federal contractors. People providing services to the federal government that is a six-hour reporting requirement. It is complex, it can be overlapping, but you have a lot of cooks in the kitchen. I think there are efforts. Much of the federal government's credit, there are efforts through the recently updated cybersecurity strategy in the side implementation plan. Also, as part of CIRCIA, DHS has been tasked with sort of setting up coordination. They were tasked with setting up a Cyber Incident Coordination Council. That was looking at critical infrastructure sectors, the SEC and other reporting requirements across the federal government to see where they can streamline and sort of lessen the burden. It's complex. For organizations knowing sort of who's who in the zoo, and who you have to deal with, I think is a real threshold question that everybody needs to take into account.

Judy Jagdmann:

I would just, as an aside, I assume that that's an area where Palo Alto can be of service as well, as well as law firms, helping entities navigate what they have to report to him.

Sam Kaplan:

Palo Alto through Unit 42, they have the threat intelligence, but they also have the consultative services, which can help organizations develop risk management plans, but they also do incident response. We actually do partner with firms like Troutman, but other firms to help organizations. Because, with these reporting requirements, one of the things that we've seen in that I've seen through the regulations, cyber incident response needs to be thought of more holistically across the spectrum organizations. You need a broader set of stakeholders that are involved in responding to a cyber incident. Includes legal marketing, your C-suite should be involved, your board of directors. There's a lot of people that need to be involved in the process

to assess the severity of the incident and how to respond. This has really become an all of the corporation type of capability.

Judy Jagdmann:

Just a follow up to that in discussions with others, in this industry, we've talked about the all of government approach to cybersecurity that we're seeing. Every agency is using all authority that they have to push out cybersecurity requirements to all business entities. If you don't have a plan, I think you ought to seriously think about getting one. Because if you don't have requirements on you now, you're going to have them soon. In any event, we're all vulnerable, and we just need to be prepared. I'd like for you to comment on that.

Sam Kaplan:

I think you're absolutely correct. One of the things that we've seen accompany some of these cyber incident reporting rules, and we actually see this in the SEC rule. But also, both domestically and abroad, when you have multinationals that are dealing in this territory, there are cyber regulations across the globe. Some of the trends that I've seen, and I'll use the SEC as an example, is they will implement a cyber incident reporting requirement. But part and parcel to that is, the expectation that companies are going to have to take cyber risk management practices seriously and start reporting on how that particular entity or organization is both managing their cyber risk, how they're identifying threats and vulnerabilities, how they are operationalizing cybersecurity policies through those corporations.

I think we will see sort of these types of requirements not only on the incident management side, but on sort of the cyber risk management side continue to propagate. That is the whole leg, second leg of the stool under the SEC rule.

Gene Fishel:

Thank you, Sam. I see we're almost at a time. But just to wrap up, if I could ask what sorts of cybersecurity threats, and issues that you see on the horizon, and how can critical infrastructure companies protect themselves from those?

Sam Kaplan:

I think the threats and vulnerabilities that I sort of identified, we'll continue to see those buckets and types of vulnerabilities just continue to spread. I think, for example, if you take sort of the known and exploited vulnerabilities section, as critical infrastructure operators are continuing to automate, and network their capabilities. Their attack surface is inevitably going to grow. The more things you have networked or connected, potentially open to open Internet connections. That attack surface is just expanding by multiples.

Having the ability to understand what your attack surface looks like, understand how many devices you have connected both to a network, but through the Internet is going to be crucial to understanding and protecting your own network. This includes IoT devices. When you start looking at IoT devices, more and more corporations, organizations across the board, but to include critical infrastructure. Smartphones, connected devices, like TVs or telecommunications

equipment, it is all networked, and each one of those devices that is open to a public Internet is a potential vector for them to get in.

Palo Alto Networks has one of the more sophisticated attack surface management platforms. It's called Xpanse through our Cortex. But it can get in and really help organizations know how many points of contact they have across their networks that are facing the open Internet. So understanding that attack surface, I think is going to be crucial, especially on that known and exploited vulnerabilities.

I think the other trend that we're going to continue to see down the road is the scale and sophistication of attacks. I think we can expect to increase over the coming years. This is in part due to advances in artificial intelligence. Our Unit 42 has published sort of threat reports with regard to how ransomware actors are using generative AI systems to create more sophisticated phishing techniques to be able to penetrate those systems. This can include all the things that you've trained your organization on to look for bad grammar, and then email, or strange phraseology. Generative AI systems, which are free to use, threat actors are using this to write very sophisticated both phishing, and spear phishing campaigns that don't have all the hallmarks of traditional phishing campaigns that we've trained the workforce. I think, with regard to sophistication, I think we're going to be able to see that.

The other sort of outgrowth to that is the ability to scale those attacks, to hit numbers of systems and to sort of accelerate how they probe, and how quickly, and how large in scope they can sort of probe for vulnerabilities across those systems. I think that scale and sophistication is one of the things that we have to be continually vigilant to look out for.

Judy Jagdmann:

Sam, I believe our time is up. I want to thank you again for being with us today. This has been a great opportunity to go over some very important information. I'll just note that you and I were recently on a panel together at an attorney general's conference, and I knew you would make a great podcast star for us, and you've certainly delivered today. So thank you, again.

Sam Kaplan:

Thank you again for the invitation.

Stephen Piepgrass: Gene and Judy, thank you for sharing your conversation with Sam. I'm certain that much like myself, our listeners enjoyed your candid remarks and invaluable perspectives.

I want to thank our audience for tuning in today too. Please make sure to subscribe to this podcast using Apple Podcasts, Google Play, Stitcher, or whatever platform you choose, we look forward to having you join us next time.