Stephen Viña:
I'm going to take you back to around 2017. Russia wanted to take down certain government operations in the Ukraine. Russia was looking for different ways of how they could cause damage to different operations within the Ukraine. They decided to infiltrate a software company in the Ukraine, and they were able to put in malware into an update of this particular tax software. If you were doing business in the Ukraine, you had to have this particular software. When that software was uploaded and patches were implemented across the software, you also took on and downloaded this malware. The impacts were not only in the Ukraine, but across the world, and we saw, overnight, companies taken offline, impacting global operations across multiple companies, including here in the United States. This was a real wake up call to companies and to nations of the extent of the damage that could be done by a cyber attack.

Erick Gustafson:
This is the podcast This Moment Matters from Marsh McLennan, sharing the expertise of our four businesses, Marsh, Guy Carpenter, Mercer, and Oliver Wyman. I'm Erick Gustafson. Today's guest, Stephen Viña, served as chief council for Homeland Security under Delaware senator, Tom Carper. This was back in 2011 when he worked on a cybersecurity framework, the best practices for organizations to avoid getting compromised by online criminals. He's from Edinburg, Texas, which is next to the US-Mexico border, went to law school at Texas A&M, and right out of school was working on Capitol Hill. It's an interesting path from there to Marsh where he's now a senior vice president in our cyber practice. In my discussion with him, we started at the ground level, one common way that hackers actually break into organizations.

Stephen Viña:
When you think about that a simple phishing attack or some type of email social engineering can literally cost your company hundreds of millions of dollars because of a ransomware event. I work in cyber claims now. I see this every day. Organizations, through some type of social engineering event, clicked on a link and within minutes, millions of dollars out the door, spent on not only just the ransom itself, but on remediation, on forensic, on legal expense, on data recovery, on reputational damage, and then not to mention even potential litigation and all those third party costs. Regulators, asking questions. There's so much writing on this that I think people forget that they have a responsibility to improve their awareness about cybersecurity and working with their organization as well as they are part of the solution to address this risk.

Erick Gustafson:
That's a great point, and it is frankly easy to forget each of us has that responsibility. I want to circle back to the story we started the podcast with, on the break in in Ukraine. This was a real wake up call to companies and to nations about their vulnerabilities, but it was also a bit of a wake up call for folks that wanted to engage in criminal behavior. Can you tell us more about that?

Stephen Viña:

Absolutely. I think we're starting see this blurring of the lines between nation state activity and criminal actors sometimes working at the behest of a nation state, sometimes working just in tandem or at the actual direction. But if anything, at the acquiescence or the blind eye of a nation state, but the end result is the same, in that there is a constant and persistent and severe threat against our businesses and other organizations every day, every minute.

Erick Gustafson:
One of the things that has come to light recently is the need for collaboration between governments and the private sector. It's a little bit of a challenge because there has been a lingering tension between regulators and cyber hacks, right? Where it's almost a blame the victim mentality. But one of the ways that we can improve resilience is greater collaboration. As someone who worked in government, how do you see the collaboration improving? What should businesses be doing, what should governments be doing to work together more seamlessly?

Stephen Viña:
No, that's a great question. There's this inherent tension at times, or at least a perceived inherent attention, between government and the industry, as oftentimes as regulators or as enforcement actions that may be burdensome companies are sometimes reluctant to cooperate and collaborate with the government. But I think what we're seeing here with the onslaught of ransomware attacks is a necessity that is needed for cooperation and collaboration and coordination across industry with government, with nonprofits, an all of the above approach to tackling this problem. Because we're dealing with nation states with sophisticated criminal organizations that may have the backing of a nation state, and so there's multi-pronged approach, and part of that is industry coming together, working with each other and working with the government, sharing best practices, sharing threat information, and sharing other data that's necessary to get a real understanding of the severity and the totality of the events so we can formulate better comprehensive plans to do something about it.

Erick Gustafson:
If I'm a company, right? And I have exposure, or if I have been hacked, do you know how to advise the company to engage the government? What sorts of things should they share? Is there an 800 number? That sort of thing.

Stephen Viña:
Well, there's several probably ways to have contact with the government. First, I think if you're a regulated industry, you might have that relationship with your regulator, and the Department of Energy is a great example, where they have a whole cybersecurity office. They have different operations set for their industry. Financial sector's another area where they have particular industry resources that maybe they even sit together in Information Sharing and Analysis Center, in ISAC, S-ISAC. The Department of Homeland Security is the quarterback and the coordinator for industry cooperation, and they can provide valuable resources as well. But usually, in the event of an actual attack, one of the first points of contact are often the FBI local field office or even the Secret Service local field office as well.

Erick Gustafson:
Stephen, your background working on Capitol Hill in a variety of capacities at the Congressional Research Service, on a committee, on the House side and ultimately on Senate side, really is a unique preparation for your work at Marsh. Now, so much of the cybersecurity landscape is still coming together, the ways that governments work with other governments, the ways that businesses work with government. What can you tell us about your experience in public policy and in the government as to how we should be thinking about enhancing those partnerships?

Stephen Viña:
Sure. I've worked in Congress for nearly 15 years, first, as you mentioned at the Congressional Research Service, which is like a think tank for Congress. There, you really get to take a deep dive into issues and understand litigation that may impact legislation and how members are approaching issues. One of the things about CRS, it's nonpartisan. You're really trying to just cut right through the left and the right and tell how it is down the middle. On the House side, I really got an understanding of a variety of issues working with state and locals, getting those perspectives, working on counter-terrorism issues and border security issues, and then of course in the Senate, we're really focused on cybersecurity and understanding working with industry privacy groups. All the different constituencies that have an interest in these issues, including law enforcement and national security perspectives.

Erick Gustafson:
Yeah. All the stakeholders.

Stephen Viña:
Really put those interests together is how you move a piece of legislation. We worked day and night to pass several bills, including an information sharing bill that provided certain liability protections for industry who shared cyber threat indicators, and that's one of the tools in the toolbox right now for S-ISAC and other agencies working with industry. But I think working on Capitol Hill really helps you understand the different perspectives and the different dynamics that are behind cyber legislation and cyber policy, and just how challenging it is to bring the parties together to find a bill that will eventually pass and become law. Then that was one of the issues that I was dealing with, in particular around 2014, 2015, when we were trying to pass legislation that created more of a regulatory framework for cybersecurity, and those discussions are ongoing right now. But those discussions back in 2014, 2015, we were not successful in passing that regulatory bill. What came out of that was the Cybersecurity NIST Framework, put forward by the Obama administration. That framework was voluntary guidance. The framework was drafted by the NIST, National Institute of Standards and Technology, and it was put together with the input of industry. They had a seat at the table developing these voluntary standards. The question became, well, how do we incentivize companies to adopt these voluntary guidance and standards? One of the thoughts was, well, maybe insurance and cyber insurance can play a role in that. My boss, at the time, wanted to learn more about that issue. That's where I really started doing a deeper dive on cyber insurance and cyber risk management, and that ultimately led me to Marsh.

Erick Gustafson:
I'm interested in insurance for many reasons, but I think it has this unique social mission, right? Where the insured party doesn't want to ... If you have auto insurance, it doesn't mean you want to have a car crash, right? The manufacturers of the cars are trying to do things to make them safer, and clearly insurance carriers don't want to see you have a car crash either. Everybody's incentives are aligned in order to have safer vehicle, right? A better experience driving. I think you can take that model and apply it to how society prepares for earthquakes, hurricanes, and yes, cybersecurity. Can you talk to us a little bit about what some of the outcomes have been of the framework, ways in which working with companies like Marsh have improved their cyber hygiene?

Stephen Viña:
Sure. I think for leading companies, it's those that have embraced cybersecurity as a business enabler, companies that have embraced that kind of strategy and see cyber as really a market differentiator, a place where they can really separate themselves from their peers. I think those are companies that are set up for success in the long run. What we see is, with the NIST Framework, companies that are using the framework, and if you take a step back, it encompasses the life cycle of a cyber event. We're talking about taking measures to identify, protect, detect, respond, and ultimately recover from an event. It really sets some guidelines for companies using best practices that they can measure themselves and say, "Okay, what's our target? Where do we want to be and where are we now? Then we can dedicate resources and reprioritize as needed given the impacts of the day and the threats of the day." They can really make some decisions, some risk management decisions, to better align their resources with their risk. I think the NIST Framework has really helped companies talk a common language, it's helped them identify gaps and measure priorities, and it's helped them improve their cyber hygiene all around because now they have a whole set of best practices at their disposal that they can choose from.

Erick Gustafson:
Man, has a lot changed in just a short period of time and in the online world. Let's talk about the advent of the ransomware period or time. Can you maybe give us a little bit of a sense what is ransomware, and then talk to us about how it came to be that it is now everywhere on the front page of magazines and newspapers?

Stephen Viña:
Sure. Ransomware is a type of malware that's used by, in this case, particularly criminal organizations, but nation states as well, that encrypts your data. Then to get a decryption key, you have to pay a ransom or an extortion. In a lot of cases now, we're seeing what we call a double ransom, in that the hackers not only encrypt your data, but they also steal it too. You're being extorted for the decryption key as well as potentially a release of your data. Ransomware is a type of malware, has evolved over time to the point where now it's almost a service that bad guys can find in the dark web and are able to really turn on very quickly and inflict damage across to the world. Really they're kind of shooting almost like a shotgun trying to see whatever

they hit, and then from there, they're looking for open doors, basically, across organizations. And when they find one, then they infiltrate the company and that's when they start poking around. They might find the data that's the crown jewels, so to speak, and they take that data and then that's when they launch the ransomware and actually encrypt your files and say, "Oh, by the way, we have your data here and we're going to release it to the general public if you don't pay us millions and millions of dollars."

Erick Gustafson:
We have seen cyber attackers take control of physical assets or disable their use. It's not just data, right? It's the capacity for systems to operate. Unfortunately, no system is perfect, right? You're not going to keep every criminal out. Is there a way that companies can lower their exposure to something that might be inevitable for them?

Stephen Viña:
Right. You mentioned the physical part of it, and I think that is the worry for particularly government officials, but obviously for communities and for organizations and companies that run these utilities. The threat of moving over from the corporate network to the actual operational technology and being able to manipulate industrial control systems in a way that might impact a community. We've seen examples in a water treatment plant in Florida. There was examples about a dam in New York and other types of critical infrastructure here in the United States. At least, it appeared that some type of outside organization or outside entity got into the control systems and was able to manipulate some of the terminals. Luckily, nothing came of those issues and they were quickly identified and remediated. Again, it's another wake up call that it's not only talking about corporate IT networks, we're talking about industrial control systems. In many ways, those industrial control systems, they're legacy, they've been around for 20, 30 years. Updating and patching those systems is more challenging. The vulnerabilities are there. I think that is a key issue that I know, again, government, industry and others are very concerned about.

Erick Gustafson:
Both in terms of data and physical assets, Stephen, how should companies prepare or anticipate attacks that could affect not only their data, but also physical systems?

Stephen Viña:
Well, every company's different. Again, it's part of their risk management strategy. They need to assess their people, the process and their technology, and they need to identify where there might be some vulnerabilities and where they can strengthen and improve. In many ways, again, I'm going back to that NIST Framework, there's a variety of best practices there. But just for example, right now when we're talking about ransomware, I know from an insurance perspective, the insurers, they want to see multifactor authentication throughout the organization, particularly for administrative privileges. They want to see better access management and control tools available. They want to see endpoint detection monitoring. They want to see an incident response plan. Not only that you have one, but that you've tested it. They want to see a strong vendor management program, a patch management program as

well. There's a variety of different tools and techniques out there that organizations are doing, and they should probably be doing more of. Backups and recovery is also a major issue right now, particularly with ransomware, is one of the methods of best practice to make sure if you are a victim of a ransomware event, is to be able to restore your systems from your backup recovery data and systems. A lot of organizations, they may not test that backup, or they may think it's airtight, but it's really not. I know from an insurance perspective, they're definitely asking questions about, well, what is your backup strategy? How often is it completely offline? How often do you test it? Basically, they want to know if you take a punch, how fast can you get backup?

Erick Gustafson:
Right. Right. Insurance companies and other risk advisors are driving the progress to some degree. What maybe is in the future? What kinds of tactics might be in the offing, apart from multifactor authorization, as well as air gap, backups and things of that nature?

Stephen Viña:
I think we're seeing a real emphasis on cyber threat intelligence, really understanding what you're up against and the threats that are coming in so you can make better informed decisions to move and be flexible for those threats that are coming in. Another area of emphasis that I think organizations, you'll see a lot more efforts behind is training and awareness. I think the people, oftentimes, they say are a weak link. I think that's why you see a lot of emphasis on training and awareness, whether it's phishing testing or just general awareness and understanding the threats that are coming in. Social engineering types of threats are very real, and they're often one of the major ways that ransomware malware is inserted into a network, because the bad guys have become sophisticated enough where they understand what you might click on, and so they'll craft a message that looks so real that you, on a long day, may just click on it, and then from there, the hackers are able to get in. Remember, the hackers only need to be right one time, organizations have to be right all the time. They're playing those odds. Awareness and training is going to be a key factor moving forward.

Erick Gustafson:
Definitely is. I'm paranoid every time I get an email from something I don't expect. I just look at it, I study the bottom of the signature block of whoever sent it. If I don't know the person and I'm not familiar with the service, I'm not clicking on the link. It'll be interesting to see how marketing evolves given the general paranoia that has come around.

Stephen Viña:
Well, you asked earlier about some kind of evolving threats and what's on the horizon and the question about how marketing might evolve. Right now we're seeing this evolution of deep fakes and misinformation, and we're seeing it really in the political sphere and celebrities. It's oftentimes you put the head on a body of someone else and pretend like they're saying something. But this technology is getting backed by artificial intelligence. AI is getting very, very real. We are seeing that in the criminal world and organized crime, where they're able to manipulate, of course, letters and signatures and other corporate data, as well as now voices

and of course images. They're really able to fabricate a whole story out of thin air, just to get you to click on a link, to authorize a payment, to move money around. Of course, it's not you, it's fraudulent. But this is what the hackers are doing to somehow make money.

Erick Gustafson:
Is that something that multifactor authentication can defeat, or where does that ... I would imagine if you're a hacker, right? You're trying to come up with a new technology that isn't going to be easily blocked or defeated by MFA or something that is training, that is already in the training ethos of a company or a carrier that might require it. How might these interesting innovations that the hackers are coming up with drive new training technologies, new forms of security? What are your thoughts about that?

Stephen Viña:
When you think about cyber threats, I think one of the frameworks is looking at it through the impacts it'll have on the confidentiality, the integrity and the availability of your data. Confidentiality, of course, is we've seen those types of threats for a long time related to data breaches and the actual exploitation of important information. The availability of data. We're seeing that right now with the ransomware events. They're locking up systems and preventing you from carrying out your day-to-day activities. What we haven't seen a lot of is attacks on integrity. I do think this is something that we have to watch out for as companies and organizations and as a nation too, because I think this is where we'll see an evolution in the different types of malware, putting into question the integrity of the data that's in front of us. From a corporation, maybe it's their 10K and other annual. If hackers are able to manipulate that data and then maybe extort you by just threatening that they had done a certain manipulation of the data. That could be a major risk and consequence for an organization. I think the integrity issue is one to watch for, and I think there's some companies out there that try to help bring some authenticity and they compare the pictures and they're able to basically validate whether it is authentic or not. I really think we'll be able to address those types of threats.

Erick Gustafson:
Stephen Viña is senior vice president of Marsh's Cyber Practice and an adjunct professor at American University. If you want to learn more about Marsh McLennan's work to enhance cyber resilience, visit mmc.com. This Moment Matters is produced by Marsh McLennan with Connected Social Media. I'm Erick Gustafson. Thanks for listening.