The Economic Club of New York

115th Year
665th Meeting

Shawn Henry
President and Chief Security Officer
CrowdStrike Services

June 14, 2022

Webinar

Moderator: James A. Hasso
Managing Director, Voya Financial

Introduction

President Barbara Van Allen

Good afternoon and welcome to the 665th meeting of The Economic Club of New York. I'm Barbara Van Allen, President and CEO of the Club. It's an honor to be here with all of you in our 115th anniversary year. So we have lots to celebrate, considering we've been around now for more than a century. The Economic Club of New York is the nation's leading nonpartisan forum for discussions on economic, social and political issues. As many of you know, we take no position on any issue. We've had more than 1,000 prominent guest speakers appear before the Club over the last century and we have a very strong tradition of excellence.

A special welcome to members of the ECNY 2022 Class of Fellows – a select group of diverse, rising, next-gen business thought leaders, and students joining us online today from the CUNY Graduate Center and Rutgers University.

It is really a pleasure to welcome our guest today, Shawn Henry. Shawn serves as President and Chief Security Officer of CrowdStrike Services, leading a world-class team of cybersecurity professionals in investigating and mitigating targeted attacks on corporate and government networks around the globe.

Under his leadership, CrowdStrike engages in significant, proactive and incident response operations across every major commercial sector and critical infrastructure, protecting organizations' and governments' sensitive data and networks around the world.

Shawn's work includes educating boards of directors and executives of key companies on critical proactive security measures, governance, and corporate readiness in the event of a breach. He also oversees all security aspects of global CrowdStrike facilities, personnel, executive protection, and corporate events. He joined CrowdStrike in 2012 after retiring from the FBI where he oversaw half of the FBI's investigative operations that included all FBI criminal and cyber investigations worldwide, international operations, and the FBI's critical incident response to major investigations and disasters.

He also oversaw computer crime investigations spanning the globe and received the Presidential Rank Award for Meritorious Executive for his leadership in enhancing the FBI's cyber capabilities. Shawn lectures at leading universities and he's a faculty member at NACD to which many of our members belong. He serves as a keynote speaker at major cybersecurity conferences around the world and is regularly interviewed on cybersecurity issues, as you can imagine, by major broadcast, cable, online, and print media.

The format today will be a conversation and we're very fortunate to have fellow Club member and Managing Director of Voya Financial, James Hasso, as our moderator. If you do have questions, please put them into the chat box and time permitting, James may bring those forward. We will end promptly at 3:15. Any questions submitted to the Club from members have already been shared and might be addressed during the conversation. As a reminder, the conversation is on the record and we do have media joining us today. So without further ado, James, the mike is yours.

Conversation with Shawn Henry

JAMES A. HASSO: Thank you and good afternoon all. Thanks, Shawn, for being here. And, of course, thank you for spending 45 minutes with us to hear about the cyber world. You know, I think one of the opening comments we'd like to hear your thoughts on is the emerging cyber threats that are occurring both here and globally and how they're influencing decision-making from the government level to the corporate level, and kind of set the stage there and we'll go from there.

SHAWN HENRY: Well, thanks, James. And thanks, Barbara, and the ECNY. I really appreciate the opportunity to be here to talk about something that is really important to me because I really see it as a significant threat, and in some cases an existential threat where nation states, organized crime groups, hacktivist groups, terrorists are utilizing

the cyber threat vector as another way to achieve their objectives.

So, you know, James, when you ask about the emerging threats, what we're seeing is built on more than 20 years of expertise that different threat actors have developed. And I, you know, I mentioned a couple of the groups. Probably the two most significant are nation state adversaries and organized crime groups. From a nation state perspective, we've got what we call the Big Four – although there are dozens of countries that have very specific electronic espionage capabilities – but China, Russia, Iran, and North Korea are the four that are the most prolific, the most active, and the most capable. We see these nations targeting other countries for a variety of reasons, as you might imagine.

And some of the things, the topics that ECNY talks about, global issues, geopolitical issues, social issues, these actors are using the cyber vector as a way to amplify their voice, a way to change people's minds on certain things, to exfiltrate very sensitive intellectual property, which they then utilize for their home nations, to make them more competitive on the global stage. And what we're seeing, really in the last couple of years, are disruptive and destructive attacks. So we're seeing nation states launching these types of attacks. I'll talk about them in a minute.

Disruptive attacks are, probably the best example is ransomware. And everybody that's

on this meeting has heard about ransomware attacks which have crippled major companies and cities around the world, municipalities that have been shut down for days or weeks or in some cases months. Whole portions of the cities shut down because an adversary launched malware that encrypted the data residing on the target network. And unless you were to pay a million dollars, $5 million dollars, $30 million, we've seen some ransom payments, you don't get access back to your data because you're not able to decrypt the data. Those types of attacks called disruptive for obvious reasons, but really are utilized to gain revenue for these organized crime groups.

Nation states have used them as well. We've seen North Korea utilize ransomware to raise money because of global sanctions. They've launched ransomware attacks, other types of attacks and have acted almost as organized crime groups have with a very clear financial motivation. They are looking to generate revenue and they're using this, this attack vector because it's easy to do. It scales very easily. In many cases, it can be done in a somewhat anonymous way. There's certainly at least an arm's length capability to remove yourself from the target of law enforcement or other nations. You're able to hide your activity oftentimes. So those types of attacks, these disruptive attacks are a major issue.

The last piece I'll mention, James, is the destructive attacks. And I mentioned that nation states have utilized destructive attacks. We've seen three foreign governments

that have launched destructive attacks inside the United States against the commercial sector. And when I say destructive, I'm talking about an electronic attack that actually physically alters hardware so that the hardware is rendered inoperable.

So imagine desktops and laptops and servers where the data might be destroyed or rendered inaccessible, but also the hardware is altered in such a way that you can't boot it. You can't start it up and utilize it. So in order to reconstitute your environment, you actually have to bring in new pieces of hardware and rebuild the physical infrastructure. So Iran, North Korea, and Russia have all launched destructive attacks against the commercial sector inside the United States. That, to me, is a major concern when I'm thinking about emerging threats, where things are headed, and what the potential significant implications might be, not just on companies but on society as we know it.

If you think about a destructive attack against critical infrastructure, for example, against the electric power grid, we've seen Russia, as part of the Ukraine war, launching destructive attacks against critical infrastructure, turning the lights off, really turning the lights off. And that is a major concern for Americans. It should be. The Department of Homeland Security has put out, just recently in the past few weeks, alerting to the United States, to critical infrastructure, saying put your shields up because there's a concern that Russia might strike with a destructive attack or a disruptive attack inside

the boundaries of the United States, perhaps to compensate for economic sanctions.

So these are major concerns. Anybody that's in business, you don't have to be a cyber person to be concerned about this. Anybody who relies on the internet, and I presume everybody in this audience relies on the internet on a daily basis, probably most of us more frequently or more regularly than we'd like to actually. But that's a very quick snapshot for you, James. There's a lot more to talk about.

JAMES A. HASSO: Well, just, I'm building on that as we look at Ukraine and Russia, China and Taiwan. You mentioned North Korea, Iran, etc. As you look across the ecosystem and what is going on and what could be attacked, what is most vulnerable within our ecosystem? So put aside government, we talked about the grid, but when you look at the private sector, the commercial sector, what areas do you think they could target which could be detrimental, not only to government but to the commercial sector as well at once?

SHAWN HENRY: Yes, well, I think when you're thinking from a security perspective, right, so I'm focused, I was focused in the FBI on investigations to try and identify who would launch these types of attacks or who did launch these types of attacks. On the commercial side, I'm in a proactive and a preventative posture. And when you're thinking about security, you've got to think about who would target you and why would

they target you. It helps you from a defensive posture to be more capable to prevent these types of attacks.

So when I'm looking at Russia, why might they target the United States? Well, they might target the United States because of sanctions. We've seen other nations, Iran, for example, launched a denial-of-service attack against the U.S. financial services sector in 2014 - 2015 based on economic sanctions that the U.S. levied against Iran. And when we're looking at Russia, you've got to ask yourself, why would they target the U.S. and if they're looking to impact the U.S. on the heels of sanctions, what sectors would they target?

And the financial services sector is absolutely a sector that will be targeted because they want to take retribution. They want to bring some pain to the U.S. and not just the U.S., by the way, it's the entire western civilization because this is clearly a global response for the war in Ukraine and there are countries around the world who have levied sanctions. The economic engine inside those countries are a potential target.

We're also looking at energy as a target. You know, 70% of Russia's GDP is based on energy and U.S. companies and western companies that are competing are potential targets. We've seen Russia target the energy sector in the U.S. in the past, not necessarily with disruptive attacks but theft of intellectual property, looking at where

companies are looking for energy, how their manufacturing facilities, what they're doing as part of the processing of energy, where they might be looking for oil and those sorts of things. So those are two of the sectors.

But it goes beyond that because any commercial sector that is somehow of importance to the United States, they are potential targets, and quite honestly, we've seen Russia attack specific individuals or specific companies and there have been many companies that have been ancillary damage. They were collateral. They were not the intended target, but because of the way malware transfers through the internet, other companies that weren't even targeted suffered and were hit significantly.

There was a major attack going back several years now, 2016, called NotPetya, that was launched by Russia against Ukraine, four or five years ago. And there were U.S. companies that suffered because of how they were connected to that targeted entity and it cost $10 billion around the globe. This is a major concern for us.

And if we've got more time, I'd be happy to chat a little bit about China because as I'm looking forward, you know, we've seen Russia/Ukraine and people were somewhat reacting to that, but I think if we're looking at China/Taiwan, I think we should be thinking about what that looks like and how does that impact all of U.S. commerce because of how the United States deals around the world.

JAMES A. HASSO: With that said, you talked about disruptive versus destructive and how these cyber-attacks, because years ago cyber packages were bought by technology groups within companies, they were bolted on, everybody used similar products, etc. Now, as you point out, there's multiple threats and they're coming from all different angles so these packages have to be customized. How do you bring together the operational and the informational side of the technology to make sure I'm not destroying company servers and also I'm not hacking in and getting Social Security numbers? How do you create that package so customers can feel safe that, one, they may not be bankrupt, because if you destroy their equipment, they may actually be a bankrupt company at the end of the day, not only a company under siege?

SHAWN HENRY: Yes, so I mean from my perspective, from a security posture, first of all, companies are responsible for protecting their own networks and their own data. In other words, in the physical world, we expect that the U.S. government protects us from an incoming missile or an incoming aircraft that's carrying missiles, right? We expect that the Air Force and U.S. forces are going to respond and protect us. You and I don't have in front of our house anti-missile defense systems and we don't have our own fighter jets.

In the information technology world, it's not the case. The fact of the matter is the U.S. is not putting NSA into the ISPs to filter out all the malicious traffic, which means that

every company is going to be responsible for protecting themselves. What that means is you've got to have the right technology and the right capabilities, and I think U.S. companies are starting to get that. I think boards of directors are starting to invest. They recognize the risk. They recognize it from a financial perspective, from an operational perspective. So companies are investing in technology.

From my perspective, it's about being proactive. The malware is changing on a daily basis and you can't, from a preventative perspective, you can't put in signatures to try and block every piece of known malware because every piece of known malware today is wonderful, but tomorrow there will be 50 new pieces of malware and the day after that and the day after that. It just continues. So what you need to do is have technology that is able to identify malicious activity, not necessarily malicious pieces of software using signature. So that's one of the things we do is really look for the anomalous behavior in an environment and be able to identify those tactics and techniques that adversaries are using. And then if you can disrupt them, identify them quickly and disrupt them quickly, you can mitigate the impact of an attack.

So I think it's really about companies being more proactive. It's about them understanding the overall risk. This is a business risk and it needs to be addressed through the whole of a company, not just by the Chief Information Security Officer, but the company needs to take it seriously and recognize that it's an enterprise issue. And

the right way to do it is having the right processes, the right policies and absolutely the right technology to help disrupt these attacks before they impact the organization and you wind up on the evening news.

JAMES A. LASSO: So with that said, we look at the public sector, we look at the private sector. And the private sector, as you point out, boardrooms are becoming more aware of how necessary it is to have the right tools in place to protect their customer, clients, etc. And then you worked for the FBI for 24 years, 10 years at CrowdStrike, now when you compare and contrast public, you know, and then private, and we look at the government systems and how they have built out their cybersecurity protocols, where do you think we are, the government versus the private sector? Ahead? Behind? Do we need to advance much quicker?

SHAWN HENRY: So it's very interesting, that question. I spent 24 years; I was focused on what the government should be doing to protect its own networks. And then beyond that, how does the government help to protect the private sector? I think I came to the realization ten years ago that the public sector, the government was not going to be able to protect the private sector with the degree of protection required. In other words, the government doesn't have, in many cases, the capacity, the capabilities or the authorities to protect the private sector the way it needs to be protected.

I think the government, while there are many, many, and I've worked with them and there are many that are still in government, women and men who are working really hard. I think the framework that's currently in place doesn't allow for the flexibility, the speed by which changes need to be made. And I just, I knew that the private sector was going to have to protect the private sector and actually ultimately the public sector. Right? I mean companies like mine are using our technology inside the government, multiple governments around the world to help protect them.

So, you know, I think the folks in the private sector have come to that realization that you're not going to put the digital equivalent of an anti-missile system inside your house. So you're going to have to invest into the appropriate technology. There's ways that the government can share intelligence that can help them actually identify who the actors are and mitigate them that way. That's probably a topic that's a little broader than for this particular call. But there are ways where the government and the private sector should be working together.

JAMES A. LASSO: And on that note, when you think about the financial services sector, right, as you look at, it can go on within that sector very quickly. Seizing ATM machines, hacking into servers, proprietary data sits in those banks across the country. And when you think about what they're doing to protect their system, many of the largest banks in the country have talked publicly about their cyber protocols, cyber teams, etc. But we

have several thousand financial institutions in the United States. How do they work together to make sure collectively they're sharing information? Because that is one of the things that I believe is going to be most important moving forward, is telling your neighbor you were threatened. It's like the camera, the Ring camera. How do you do it in the cyber world?

SHAWN HENRY: Well, I would say first off that while it's the most targeted – I think the financial services sector is the most targeted – they also, the financial services sector has probably the most robust and most capable cybersecurity program, if I'm looking at all of the different sectors. You know, healthcare and energy, communications, transportation, etc. I think financial services has the best, probably because it's the most targeted. That's one reason.

The other reason is because you can pretty easily quantify what the loss is in the financial services sector. In other words, if somebody breaches a bank and is able to implement some type of an ACH transfer because of the access they've got, you can quantify what that loss is. Versus, you know, a manufacturing company that loses intellectual property, it's a lot harder for people to see it and understand it. But, you know, if there's $5 million missing from the bank, pretty much everyone knows the loss starts at $5 million and goes up from there.

The sharing of intelligence by the financial services sector is another area that I think is probably the most robust. You know, the FS-ISAC, Financial Services ISAC, I've worked with them over many years, and I think, again, because it's been the most targeted sector, there's some really very, very capable people that are part of the FS-ISAC, but more importantly part of the broader security protocol within the financial services sector. I think they've got a good program for sharing and sharing expeditiously.

I think that in many cases historically organizations have been reluctant to share intelligence. They're afraid of what it might mean to them. Is there a regulatory issue? There's been some concerns in the past by different regulatory organizations that the sharing of intelligence is a bad thing. I think that's wrong, but there have been concerns expressed about competitiveness, non-compete, etc. I think that they've been the best. They've been the most robust and the quickest. That said, the best way to defend a network is speed and visibility. You have to have speed and visibility. You have to be able to see what you're defending so that you can identify anomalous adversary behavior and you have to quickly respond to it.

And when I say quickly, I'm talking about minutes and maybe hours and through some of the sharing protocols that you're talking about, James, it might be days in some cases before something gets shared and that might be too slow. So again, while I think

that overall it's a great protocol and a great strategy, it's got to be done at the speed of the internet and not at the speed of a phone call.

JAMES A. HASSO: Right. And with that said, as you talked about sophistication of these attacks, multiple countries coming at the U.S. in general but also the private sector, talent is hard to come by at times as it relates to different sectors, industries. As we know, the United States has a shortage of employees across multiple industries currently. How do you retain your talent? You have a great group there now and you have to build it out further. You have to continue advancing and compete with, one, your competitors, but also government as you point out, as they continue to advance and hire talent. Is it just compensation or other reasons?

SHAWN HENRY: It's definitely not just compensation. And I was out at RSA in San Francisco, which is probably one of the top two cyber events in the U.S. every year, and I was talking to people from the government because honestly they're losing more people than they can hire because of compensation. However, you know, I came from the government and I was in the government not because I was being highly compensated. I was there because I was part of the mission and that was something that was incredibly important to me. I decided I was going into the FBI when I was a senior in high school. That was my goal. And everything I did from that time until eight years later when I went in as a 26-year-old into the FBI and achieved that goal of mine,

everything I did was focused on getting in. And it was because of the mission.

And when I talked to these folks from the government this past week, I talked about focusing on that. You know, they were asking me the same question you just asked, how do we retain people? How do we hire people? How do we attract people? And I said you've got to focus on the mission. You've got to focus on letting people know they're part of something bigger than themselves, that they're making a difference.

You know, being able to go home at night and say, you know, that you put an IPO together or, you know, you were engaged with the PE company, that's interesting and fun. But being able to go home and tell people that you did hand-to-hand combat with three PLA from the Chinese military and you literally where engaged in that type of a fight, there's something noble about that, that you helped to protect the water system, you helped to save lives in some cases. And I know people, because of their commitment to the mission, that they have saved lives. So that's a huge protocol for the government to follow. It's what we follow every day.

I mean we are competing, major companies that are looking to hire my folks, but we hang our hat on the mission, that you're standing on the line between good and evil. You're protecting people. If you fail in your mission, bad things are going to happen to good people. And that's a really, really important issue. So, you know, compensation is

an important component, but it is not the sole component. And I would say it's actually not even the primary component. It's in the top three, but it's not the biggest component, honestly, for most people.

JAMES A. HASSO: Well, it's interesting you point that out about protecting and serving, right, because in reality people in your business today and in government who do this every day are basically, potentially saving lives to a certain degree. So with that said, I guess when you think about moving forward again, the average American now has an iPad, iPhone, etc., the protection of those goods and devices, how do you think the ecosystem can handle making sure your home is protected as well as your corporation? Because now everything is shared within your TV, within your database at home. You share your computers, etc.

SHAWN HENRY: Yes, so I want to answer that question, but I want to go back to make a final point on your last question because I think it's really important when you talked about the thousands of financial institutions, and I know folks here are engaged in this sector. You know the big banks, you think about all of the major financial institutions, the ones that are generating billions of dollars a year, them investing hundreds of millions of dollars in many cases into information security, in the scheme of things is not such a big deal.

When I think about these small, medium-sized banks around the country, it is a big deal. And when you combine that with what it takes to hire people to run the technology, to manage the technology, to stay up to speed on the emerging threats and the risks, these small institutions, they are absolutely still a major target but they don't have the resources to do it.

So a lot of these organizations are actually, are subbing out the work. They are hiring companies to do that type of work for them. They're outsourcing their security because they can't hire people and they can't train people and, quite honestly, to outsource it that way is a lot less expensive. So I wanted to make that point because you said there's thousands of these smaller banks. And I've heard from many of these, you know, local, state, municipal facilities that they're having those challenges.

When you talk about, the last question about what I call the expansion of the target space, you know, the internet of things, your dishwasher and your refrigerator, your home automation system, cameras inside your home, and honestly inside businesses as well, that are now IP-addressable, which means that they are all potentially reachable by an adversary. You know, when I was growing up, I didn't have my dishwasher connected to the internet. I still don't, honestly, between us, but a lot of people do.

And all of those devices are a potential ingress by an adversary, which means that there needs to be security protocols, both at the network layer and also at the application layer, at the device layer. And if you don't have those protocols in place, you are vulnerable and you are potentially susceptible. You know, the increase of the target space is a boon for the adversaries. It provides them many more opportunities, and it is a potential nightmare for cybersecurity organizations and for companies to try and protect.

I think that companies need to be aware that this risk is in play and that there needs to be very specific protocols, technology, policies in place to shut down those vulnerabilities so you don't provide the adversary an opportunity to exploit the environment. Because once they have that foothold, they can do a lot more damage, James.

JAMES A. HASSO: And on that note, jumping from the homeowner and the small banks, now into the public area, but actually non-financials, and one of the things that we've seen over the last couple of years especially, hospitals, nonprofits, etc. have been attacked with ransomware. Interestingly, I sit on the board of a nonprofit in New York City and we were attacked by ransomware and we basically had to give in a bit. The point being is, how do we protect those agencies and those organizations because they can actually risk lives every day. Can they afford it? Can they go and actually buy

these packages and basically support their ecosystem? Or is it that they do have to bring it in-house eventually?

SHAWN HENRY: Yes, so, you know, kind of building upon that last response I gave, I think that there are hospitals, as an example, that are investing in technology and in security. So the question becomes, anytime you're making a business decision, you've got to look at the risk that you're protecting against, what's the overall cost? What's the ROI, etc.? When we're looking at risk, do we mitigate the risk ourselves? Do we transfer the risk to somebody else? Or do we accept the risk? That's part of every business calculation. It should be a part of every business calculation.

So when companies are looking at this, they have to decide, do we buy technology that we manage and that we're responsible for, that we've got to upkeep, maintain, etc.? Or do we outsource this and transfer the risk to somebody else? Or do we just not do anything at all? I think the latter, the last choice is unacceptable. I think anybody that's looking at what's happened where whole companies have been shut down, hospitals and cities for weeks. You know the city of Atlanta, I'm not talking about little, tiny cities, the city of Atlanta, the city of Baltimore, whole portions of their constituency services were shut down, where people couldn't, you know, the judicial system, or the licensing system. So accepting the risk is unacceptable in my opinion.

So, therefore, you decide. Do we bring it in-house or do we outsource it? I think that for many organizations outsourcing is the right way to do it. We outsource lots of things, right? We don't, you know, banks don't have their own plumbers on duty or their own electricians. They're hiring people typically to come in to do jobs as they come up. You know, they hire outside counsel who are experts in certain areas. They don't maintain expertise in every area of the law. They hire people to address those things.

I think with cybersecurity, now that the risk is so high, that it makes sense for companies to be thinking about that because you're hiring people who have expertise. They've got the best technology. They've got the experience dealing with nation states all day every day. You know, even if folks in a bank, for example, have some level of expertise, they're not dealing with Russia and China and North Korea day to day to day. Maybe it's a couple of times a year. You can't stay on top of all of the capabilities, the tactics and techniques that those adversaries are using and be effective.

I think it's a decision every company needs to be thinking about. I think there are lots of options out there. And again, for most organizations, or many I would say, that's a reasonable solution and it will resonate with investors. It will resonate with the insurance company. And certainly it will resonate with the board of directors.

JAMES A. HASSO: Shawn, I'm just curious. From your years at the FBI, again now CrowdStrike, I think one of the things you brought to CrowdStrike is your expertise from

the FBI, right? Dealing firsthand with these threats that were hitting government institutions, the government in general. Do you think, when you look back, I guess the ten years at CrowdStrike versus 24 years at the FBI, what is, I guess, one of the situations that you were in that you can share, from A to Z? You had the problem and you remedied it. And no names of course, whatever you can share would be helpful and just kind of your experience on how it began and how it ended.

SHAWN HENRY: You know, I started in the late 90s and a lot of what we're seeing from nation states now I saw in the late 90s. So it's not a new phenomenon. The public is hearing about it in the last five or so years, but it's been going on for probably 25 years or more. But I remember on the criminal side, the denial-of-service attacks against retailers, online retailers.

And this goes back to 2000, even before 9/11, the big concern was those types of attacks. You know, the Love Bug attack, these viruses that were disruptive to companies. You know, a denial-of-service attack, a website defacement, and a virus like the Love Bug today, I mean those things are crumbs compared to what we're facing. So when I'm thinking about, kind of the growth of this risk, the significant capabilities that have been developed by adversaries, those are the things that concern me.

One of my first cases that I worked was, this is public, it was RBC, the Royal Bank of

Canada, that was breached, where the adversary was able to get inside the corporate network and they were able to change the permissions on ATMs. Where it's limited to $400 or $500 a day, they were able to change the permissions so they physically had people standing at ATMs in cities around the world withdrawing cash, in some cases until the ATMs themselves ran out of cash.

And now when I think about what adversaries are doing with some of the ACH transfers that they've done, I've seen banks that have lost tens of millions of dollars. Nobody physically in the bank. No actual cash, but all electronic, kind of the advent of cryptocurrency, bitcoin and others that is allowing adversaries to move money more quickly in a more anonymous way. So from my perspective over, you know, more than 25 years here in this space, it's really been how things have changed for the worse, for us, from a security perspective, but to where they're going. I think it only gets worse, to be honest. We're not going to step away from the technology. We're going to embrace the technology.

The internet, obviously it's here to stay and it's brought great efficiency and effectiveness and joy to many people's lives. So we have to manage that risk and we have to do it in such a way that allows us to enjoy the benefits and the fruits of the technology and try to avoid and mitigate the risks that are out there.

JAMES A. HASSO: So I think it's fair to say your experience at the FBI was allowing you to look forward. And as you look forward today, some of the threats that we discussed earlier, one day you see coming, including China, Taiwan, etc. And I guess ultimately, you know, not only do corporations have to step up and actually spend, but individuals, nonprofits, etc.

SHAWN HENRY: They have to. If you're on the internet, you have an internet presence, you need to have a level of security. It's got to be commensurate, of course, with what the risk is. So, you know, different organizations are bigger targets, but there are many types of attacks that are not targeted. In other words, just because you're on the network you are going to potentially suffer. So, you know, companies have to calculate this. Just like when they're doing their budgets, they think about what does electricity cost us? What does water cost us? What does rent cost us? What does personnel cost us? And what does cybersecurity cost us? It needs to be a line item in the budget because not having it is just not acceptable today under the circumstances that we're in and with the level of risk that we face. Because it is absolutely, especially for smaller organizations, an existential threat. And if we're not paying attention to it, there's going to be long suffering down the road, James.

JAMES A. HASSO: Thank you, Shawn.

PRESIDENT BARBARA VAN ALLEN: Well, thank you both. James, thank you for a serious of fabulous questions. And Shawn, very, very insightful. There is one question here that I have say I'd love to have you respond to, even if you only have 30 seconds. And that is, could CrowdStrike itself be hacked? And have you been?

SHAWN HENRY: So the answer is we know that we're a target for sure. You know, we're successfully defending companies around the world. So, of course, we would be a target. I can tell you; I am the Chief Security Officer of the company; we have a security first posture. It's something from the very first day, people come into the organization, they're indoctrinated. We've got lots of partners that we work with that help from a defensive posture. We use our own technology to defend and to identify attacks. So, yes, of course, we've seen people that have been using reconnaissance and probing our environment. That's par for the course. But it is something we are absolutely, it's our primary focus as a security company. Security is our primary focus so we take it very, very seriously.

PRESIDENT BARBARA VAN ALLEN: Okay. Well, thank you again. Excellent conversation. A reminder to all of us how important it is to have those enterprise risk management plans in place and particularly in the cyber area.

I want to just mention we have many more great speakers lined up this spring. And as

always, we encourage our members to invite guests. On June 26th, we have an in-person, that's of course, Thursday, excuse me, June 16th, we have an in-person luncheon where we'll be hosting Evan Greenberg, the Chair and CEO of Chubb. And that will be an in-person/hybrid event. Followed by Brian Cornell, the Chair and CEO of Target on June 21st, again also an in-person/hybrid event. And June 27th, we're going to have our very special Peter G. Peterson Leadership Excellence Award Dinner, where we're going to be honoring Roger Ferguson and Stanley Fischer. We bring back again the duo. July 13th, we have a webinar with Glenn Hubbard and Larry Summers. That's always very popular with our members. And then on July 21st, we have another webinar and that will be with Sarah Armbruster, who is the President and CEO of Steelcase.

And as always, we'd like to conclude with a real thank you to the 347 members of the Centennial Society, some of whom joined us today, as their contributions continue to be the financial backbone of support for the Club. So thank you, to you. And to everyone else, please enjoy the rest of your day and remember to stay up to date on your cyber protection. Shawn, James, thank you again.