CYBER SECURITY

ARE YOU READY FOR THE NEXT ATTACK?

BILL BARR

Regional Lead, Cloud Services and Security, Avanade

Bill Barr, GSEC, MCP is a Regional Lead, Cloud Services & Security at Avanade. Bill has worked in all facets of IT for over 25 years including over 10 years as an information security practitioner. From strategy to implementation, he helps clients quantify risk, understand and manage cybersecurity threats against their digital enterprises. He has worked in various industries including manufacturing, high-tech, aerospace, retail and health care. Barr has also co-authored federal government information, governance policy, technical orders and is a contributing author to several information security publications.

CHRISTOPHER ESCOBEDO HART

Attorney, Data Privacy & Security, Litigation, Foley Hoag LLP

Chris Hart's practice centers on three areas: data privacy and cybersecurity, civil commercial and business litigation, and representation of foreign sovereigns in U.S. courts and international tribunals. As founding member of the firm's Cybersecurity Incident Response team, Hart has advised companies - from Fortune 500 to start-ups - on a broad array of topics, such as regulatory compliance, data breach planning and response, and risk management (including cyber-insurance). He has also counseled several companies in their responses to data breaches. Hart is a frequent speaker on cybersecurity issues, especially those concerning litigation liability and general risk exposure, and is a co-editor of and frequent contributor to Foley Hoag's blog, Security, Privacy and the Law.

JOHN TURNER

Director of Cloud Security Enablement, Optiv

John Turner is an accomplished IT executive with more than 20 years of leadership and operational IT experience. As the director of cloud security enablement at Optiv, Turner's team of cloud architects are responsible for helping to ensure the successful integrated delivery of cloud security solutions. Turner plays a key part in bringing different areas of Optiv's team together to deliver seamless cross practice wins. Turner also works as part of the cloud leadership team to define Optiv's strategy and product portfolio.

Prior to joining Optiv in 2016, Turner was the vice president of product strategy at Adaptive Communications. He previously served as general manager of unified communications solutions at Aruba Networks. Turner got his start at Brandeis University building identity solutions and eventually leading the network and systems group as its director. He holds a Bachelor of Arts degree from the College of Wooster in Wooster, Ohio.

TIMOTHY LASONDE

President, NSK Inc.

With over 18 years of experience in the information technology and services industry, Tim focuses his management and technical expertise on running NSK Inc., a best in class IT Solutions provider. He is an expert in many technology fields including Microsoft Cloud Solutions, data storage and virtualization, business continuity and disaster recovery solutions, as well as communication systems and cybersecurity. Lasonde has an unmatched passion for breaking new ground in these areas and adapting enterprise technologies to the small business.

Lasonde joined NSK Inc in 2001 as an associate. He took the role of Partner and Chief Technologist in 2006 and then as President in 2008. His main mission today is to assist in growing NSK and continuing its focus on enterprise solutions delivered to the SMB market. Lasonde is responsible for managing the operations of NSK and his duties include managing the NSK staff and working with customers to plan, manage and implement strategic IT solutions designed to help customers use technology to facilitate growth. Under his direction NSK has continued to be a leading IT service provider in the metro Boston area.

The U.S. Department of Homeland Security says that all employees need to know the signs of a cyber-attack, not just those who work in the IT field. This is increasingly important as more companies move business operations online. The department stresses employees should make passwords complex, beware of phishing emails (opening emails, links and attachments from strangers) and report all suspicious activity to their company's IT department.

The Boston Business Journal's Table of Experts program provides insights into how to protect a company from a cyber-attack, why cyber security is important and how litigation is part of the new cyber-security landscape. October is national cyber security month.

Here's an edited transcript from the program discussion, which included NSK President Timothy Lasonde; Optiv Director of Cloud Security Enablement John Turner; Avanade Regional Lead Cloud Services and Security Bill Barr, and Attorney in Data Privacy & Security at Foley Hoag Christopher Escobedo Hart.

Boston Business Journal Market President, Publisher, Carolyn Jones moderated the discussion.

From left, Christopher Escobedo Hart of Foley Hoag, Timothy Lasonde of NSK, Bill Barr of Avanade, and John Turner of Optiv.

CYBER SECURITY: IS YOUR COMPANY PROTECTED?

BBJ: What's your definition of the cloud and cyber security? What's the importance?

BILL BARR: Cyber security is about protecting your digital assets wherever they may be. That's both your information and information about you. Information about you is already in the cloud somewhere. Think of your medical records, your banking records. You've been using the cloud for a very long time. If you have a social media account or a web mail account you're already using cloud based facilities.

CHRISTOPHER HART: I'm a litigator and ... when I'm thinking about the cloud, I'm thinking about liability. In general companies and organizations have to be concerned about protecting personal, confidential information, however that might be defined by the relevant regulatory or legal authority. And I say personal confidential information very broadly. That could include personal health information; it could include financial information. When we're talking about the cloud, all of a sudden we're talking about data that exists in a place that's different from where it originates and that can be accessed ubiquitously. Essentially, you're adding another part and another location, speaking as a lawyer not as somebody who's technically proficient.

BBJ: So, let's talk a little bit then about what are some of the most common cyber threats that businesses need to be aware of.

TIM LASONDE: So, there's phishing attacks. Those are basically people that are sent (emails), trying to get you to click on a link (or to) go to a website that downloads information on your PC. It's a very targeted attack. And then the next most common one is something called ransomware. We see that happening as well. Ransomware is when they take control of your computer. You go to a website like for UPS and you click on a link and then it downloads some malware on your machine that actually encrypts it. The real problem there is you can never get back from the encryption. So you have to restore from backup. You have to have a good recovery strategy in place. Or you pay. A lot of money in some cases. And so, those are really the most common types that we see in our business.

BBJ: What's the best approach to develop a new security strategy or when looking at what you have?

JOHN TURNER: Cyber security begins at home, honestly. One of the things that we think a lot about when we talk about training is that we train our employees how to be secure at the office. But a lot of that now is moving actually to how to be secure at home as more of us bring our work home, as more of us have digital lives and digital experiences. I think we talked a little bit about some of these phishing attacks and things like that. We always try to train employees. You've got to think about all of your social media accounts, any accounts that you have and create unique passwords. If you use the same username and the same password across all of your various shopping sites, social media sites and things like that and those become compromised or you get tricked into revealing that password and that password was used at your place of work you then create a situation where you've now brought that home threat into your employment.

BARR: The reality is most of the strategies that already exist are outdated and broken. A lot of them come from what we call bunker mentality, keeping the bad guys out. The reality is today you have to assume you've already been breached. You have to assume the bad guys are already in your organization whether you know it or not and not necessarily by any means that you may think. For example,

in terms of common attacks: wireless sniffing at public wifi hotspots or cyber cafes, device theft, even people looking over your shoulder. In terms of how you want to go ahead and design your strategy you have to start from the inside out.

The first step is to do is a very honest and candid risk and asset assessment. If you talk to most security vendors and no offense to my colleagues here, they will try and sell you a vault large enough to put your entire (business) in and some of your (business) contents just aren't worthwhile putting in a vault. So, why waste your money doing that? Find out what the important data is, find out what losses your business can suffer in a single loss. Start quantifying this and then the very first thing that you have to do is encrypt everything everywhere all the time. Encryption is the, is the very first perimeter around the data.

LASONDE: Everybody is vulnerable. Every client. Because the hackers, black hats, whatever you want to call them, they're after information. And they don't care if it comes from (a big, global company) or if it comes – from Bob's Plumbing. It doesn't matter. Those account numbers are still worth $500 on the black web. Airline miles are worth $90 per 10,000. It's big business. So, this hacking is huge, huge business. I can go right now and buy a crypto wall application and deploy it to whatever list I have and see what I get for hits and I can buy one for $80. Not only that, but from the vendor I buy it, I can also get technical support. If it doesn't work, they will give me a tutorial and show me how to use it.

HART: I had no idea. This is amazing.

BBJ: How do you pay for it? With a credit card?

LASONDE: Bitcoin. You pay for it with bitcoin (a relatively new, world-wide, electronic money form)

TURNER: The hackers they are more organized than we are.

BARR: I really want to bring this home because lots of small businesses will say, "You know, I'm a one or a two-person organization. I've got nothing anybody wants." A couple of years ago there was a small community hospital in Washington State. They had their payroll stolen. Over $1.2M was laundered through 8,000 bank accounts owned by people who had signed up for work from home schemes which were all bogus. So over 8,000 people had their bank accounts frozen. My response is you have a payroll, you're a target, simple. That's it.

HART: I think that the way that we're all talking about this is really ... as an integrated risk management problem. It has to do with customers, how you handle employee data, what your infrastructure looks like, who you hire, what your organization is. These are common ways of thinking about risk in other area, financial risk, or whatever the case may be. Thinking about cyber security as a risk management issue ... can clarify a lot of these specific kinds of problems, like third-party risk.

BARR: A couple of years ago, I had a customer who was incredibly well organized, and they'd done this exercise. I asked the CEO and the CIO the question, How much loss can you withstand, and the CEO replied, 10 cents a share.

BBJ: Ten cents a share?

BILL BARR: Ten cents a share. I said, "Great." How many of those in a row can you tolerate? (The client) said, "Three, because that affects my bonus and I lose my job!"

BBJ: Wow.

BARR: It was very simple, but they'd gone through the exercise and they'd quantified what their risk was in terms of dollars. Of course they took precautions. They had insurance and all of that. They'd already done that risk management. We didn't even talk about firewalls or end-point protection or encryption or anything. We were talking about money.

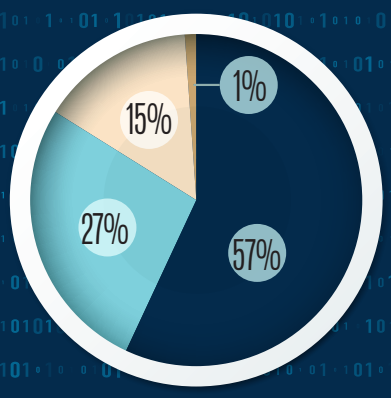
BBJ: Let's talk about a business of any size. You're giving me the advice on some things that I need to do. I'm trying to manage my bottom line and look at all the other things that I need to be concerned about to spend money on in my business.

LASONDE: The first thing that you need to do is – which costs nothing – realize that you're vulnerable. Because a lot of people don't. That's really the first step. Then once you do that ... you have to figure out where your vulnerabilities are. I think it's something that you should have an expert do who knows what to look for and knows how to present to you what they found. And then give you some strategies to mitigate that.

TURNER: We see companies engage in very risky behaviors that are really not core to what their business function is. And honestly the easiest thing to do in those cases is to stop doing that. Don't put yourself at that level of risk. Or at least be aware that that's what you're doing and if you can't spend the money, the time, the people, you know, do something else. It's important for companies to follow that comprehensive path, think about being aware of it and then build your program. Not everything has to go to a level 11. We don't need to sell you a $10M firewall today. The firewall you can get from your Internet provider may be enough to begin as long as you know how to use it.

LASONDE: Think about how you could increase your vulnerability by saying "OK, I'm going to implement a cyber

DISASTER RECOVERY



In a recent Disaster Recovery survey, we asked business owners if they currently had a Disaster Recovery Plan in place. While only 1% felt secure without one, the overwhelming majority didn't. More than 57% of those surveyed said they currently have a plan that needed a little work; 27% said they don't have a plan, but would like to develop one; and the remaining 15% have a plan that they felt was good to go.

Source: NSK

security policy" and I'm going to go get that firewall. But you don't have anybody doing management of logs. So, you think you're safe and you're not.

BARR: I see lots of intrusion detection systems that nobody even bothers to look at. It may be doing its job, but you're not getting the response value out of it. Even with the very advanced tools that we have today that involve machine learning and robotics and automation there still has to be a response to whatever alarm or alert is happening.

HART: Lawyers are important. I think all of this discussion is very valuable from my perspective in helping clients through breaches and in helping clients think about their policies. I do think that ... there's no cookie cutter approach. In other words there's no one size fits all. Make sure you have a team with the right kinds of expertise. You really do need somebody who knows how the technology works. And you really do need somebody who can manage business continuity. And you really do need somebody who's available to handle your legal and compliance issues. And I don't think that any company is going to do well if it lacks one of those resources.

BBJ: What's the future of data privacy and security? What does that look like as we go into 2017 and beyond? And perhaps any advice you want to give.

HART: I think we will be in a situation for some time where the technology is going to outpace the legal response. I think not only are individuals, courts, the legal system catching up with what's going on with cyber security issues; the technology itself is changing so much the responses to security problems, the actual awareness of what those security problems might be is in flux. I think that's going to be the case for quite some time at least from my vantage point.

LASONDE: It's important to note that information has value today and information will have value in the future and people want access to that information and that's never going to stop. We will see a lot more emphasis on end user education and training people so that they're more aware of the ways that the hackers currently get in.

BARR: It's not going to be much different with regards to the behaviors and responses. Attacks that are 20 years old still work today. People are still not doing the basics. They still aren't aware or as aware as they should be. But you have to remember whatever the good guys have the bad guys have, too.

TURNER: I completely agree. To use a cliché it's going to get worse before it's going to get better. I think over the next ten years we'll see some pretty significant breaches that will likely cause the courts to react in a particular way. It will cause governments to react in a particular way. And I think that will have some profound impact on cyber security in the next ten years. I don't have to mention names but we can think of the larger providers that exist today and the harm that could come to all of us if those breaches occur, when those breaches occur. The one silver lining in all of this is that we are all having this conversation. That's the best thing ... is that finally a broad level conversation is happening to address (cyber security).

The BBJ will have more Table of Experts programs on other topics and if you are interested in participating, please contact the BBJ advertising department at 617-316-3212.