ROUNDTABLE DISCUSSION

CYBERSECURITY

Cybersecurity issues loom large and businesses continue to struggle with the risks. What are the best strategies to stay on top of rapidly increasing threats? Delaware Business Times hosted a roundtable of cybersecurity professionals for a discussion moderated by James Collins, Chief Information Officer for the State of Delaware.

James Collins: You turn on the news, listen to the radio, read the paper, or go to any website and you're going to see an article about cybersecurity today. Why is it everywhere, in every conversation?

Scott Plichta: The internet breaks down all barriers. If you look at the threats to my house, they are limited to a couple thousand people who could actually get to my house reasonably well and try to break in. If you look at the threat to my home internet network, and a population of three billion people on the web, if even a small percentage of those people are malicious, they can get into anywhere. So, there is a subset of malicious actors or people who are just looking for opportunity. Cyber crime is just opportunistic.

James DeHoniesto

James DeHoniesto: The internet only connects us, but it's been developed with the opportunity for productivity. We're all connected. We all have our devices. We can read email anywhere, everywhere, access systems remotely. I know people who are CEOs who are looking at their security cameras from their beach house. We ensured that we can make this easy. What we didn't focus on in building this great enterprise is security.

Jim Garrity: There are no borders when it comes to the internet. People are nervous about how to defend themselves.

James Collins: What's the potential impact for businesses in Delaware?

Jim Garrity: The impact at a base level is the entire revenue stream is affected. So if I have a massive cyber attack, and I'm a technology systems integrator company, and we were attacked, our credibility in the market goes away… my business would go away, and mainly because I'm a technology company.
So it creates this fear factor. Fear leads to lack of productivity, productivity issues lead to higher costs, lower future revenues.

Jody Wilson: From an impact perspective, it's about what people see, it's about what people feel. You turn on the news and you see that there was a cyber attack or cyber security incident at an organization somewhere, and the first thing people say in their mind is, oh, I'm glad I'm not them, or, I don't want to be that.
It's the negative mentality that people see in the news and hear from the news. But let's face it, we're going to recover as an organization, we're going to bounce back. You're going to monitor it better going forward. You're going to do all the right things to make your organization a better, stronger, tighter, and more secure organization going forward. But the public's not going to see that. What they're going to react to is that you were on the news for three straight days and then you got a letter in the mail that says you're part of a credit-monitoring organization and what do they have to do, and you have just lost a significant amount of your business.
The fact is, no one wants to land on NBC 10 in the morning, and no one wants to be a part of that investigation, and we certainly don't want our organizations to be on that as well. So I think the impact really is financial…but it's also the public image, too.

James DeHoniesto: I think there are a number of organizations that believe they're too small or too specialized and they don't have to worry about this risk. Their belief is, "Not me, I don't have enough money, who wants my data, I'm just making screws and widgets, so what's the big deal?" And when you look at not just confidence, but you look at recoverability -- if you haven't planned for it -- if you haven't thought about it, if you haven't come up with your landscape on how to recover from it, you may not.

Dirk Sweigart: I have a little bit different spin on this because I come from process industries and manufacturing. I think what we worry about the most is the safety of people and the quality of life. If our infrastructure, our transportation, or if a pipeline is interrupted or compromised in some way, we worry about the safety of people, we worry about the quality of life and interruption. We think about things like floods and transportation outages and what it does to people. So we think first about safety and then we worry about productivity, production, and making sure systems run and that the information is available.

James Collins: As a business owner, what are some of the steps that I need to take to protect our team, assets, resources, and proprietary information?

Dirk Sweigart: I think the first thing you do is you put some people on it, put some time on it, some effort. You dedicate some thought to it. You need to think about what is it you're protecting and where is it and what's the real value. If you lost it, could you recreate it, do you care if somebody else has it, and what's it going to do to your reputation? If it's interrupted operation, what does that do to your productivity and your revenue?
And then once you have done that, you start looking at the threats to it. How could it be compromised, where is the greatest threat? Is it a state actor, is it someone that wants to make money from the information? Once you put those two together and you look at where your greatest risk is, you can decide where you should focus your effort. But you need to have somebody to do that and somebody that's accountable to do that.

James Collins: Can't I just buy insurance?

Dirk Sweigart: Sure, you can buy insurance, but who wants to use insurance? You will never recover 100 percent.

Scott Plichta

Scott Plichta: Insurance has now started not to pay. If you haven't put people on it and you're not doing something to secure your assets in other ways, and you're just trying to live behind an insurance policy -- there have been times where they haven't paid because a company didn't do at least the minimum to get secure. So companies have got to do something to secure their assets and protect consumer information.

Jody Wilson: For the small and medium businesses, once you know what you're trying to protect and you're ready to throw people at it, what's it worth? Because then, you need to come up with a budget line. I think a lot of small and medium businesses may not have it in their budgets or in their revenue streams to protect all of that data or can financially throwing some serious technology at it.
Identify what it's worth to the organization so it can be determined what it's going to be to protect it from that.

MEET THE PANELISTS

JAMES COLLINS, MODERATOR

Chief Information Officer
State of Delaware

James Collins is the Delaware Governor's Cabinet member responsible for leading the Department of Technology & Information (DTI), providing technology services for all state organizations. He has extensive experience as a public sector organizational leader, and private sector technology consultant; providing innovative IT solutions and implementing large-scale software projects. His achievements include expanding broadband, enterprise GIS, cybersecurity partnerships, open data portal, IT centralization, and virtualization cloud services initiatives.

He holds degrees a bachelor's degree from Wesley College and a master's degree from Champlain College in Burlington, Vermont. He served eight years in the United States Air Force.

JAMES DEHONIESTO

Director of Business Technology
SSD Technology Partners

James DeHoniesto has worked in IT for over 25 years. He is focused on Cybersecurity and Business Technology Optimization for SSD Technology Partners headquartered in Wilmington. James' goal is to ensure his clients secure their environments using practical application of current technologies and raising overall awareness of existing security risks. He also helps organizations identify the most effective technology strategies they should pursue to meet their overall business objectives utilizing existing IT resources.

A graduate of DePaul University in Chicago, DeHoniesto served in various key leadership roles with multiple publicly listed technology companies including 12 years with Hewlett-Packard.

JIM GARRITY

Chief Operating Officer
Diamond Technologies

Jim Garrity has an extensive background in service and security and functions as an information security officer for several organizations in his capacity at Diamond, including banks, telecommunications companies, health-care companies and nonprofit organizations.

Garrity is also an adjunct professor of cryptography and information security for Wilmington University, which is recognized as a National Center of Academic Excellence in Information Systems Security Education, as recognized by the NSA and the Department of Homeland Security. He has previously served in an executive capacity for companies such as Xtium (CEO), Hosting.com (VP of Hosting Services), and the National Digital Medical Archive (VP of Enterprise Solutions).

Garrity also serves on several boards including Ingleside Homes, Cr24, and Voice4Impact, providing technology and security guidance.).

SCOTT PLICHTA

Chief Information Security Officer,
Vice President
CSC

Scott Plichta has the global responsibility to protect all customer and company information.

Previously, he oversaw the development and operations of software for CSC's legal and financial services platforms. He has developed and operated SaaS platforms throughout his career, with a focus on creating software that is reliable, secure, and highly scalable.

In prior roles, he served as co-chief information officer and vice president of Information Services at Bentley Systems, and as vice president of Infrastructure Software at FirstUSA (now JPMorgan Chase). He began his career at General Electric.

Plichta holds a master's degree in computer and information science from the University of Pennsylvania and a bachelor's degree in computer science from Worcester Polytechnic Institute.

DIRK M. SWEIGART

MES Solutions Manager
Applied Control Engineering Inc.

Dirk Sweigart is responsible for the development and execution of manufacturing systems projects for ACE and serves as a consultant on information security.

Sweigart holds degrees in mechanical engineering and computer science from Penn State and an MBA from the University of Delaware. Sweigart is a member of the MESA Cybersecurity Working Group and is a senior member of International Society for Automation (ISA). He is a Certified Information Systems Security Professional (CISSP) and also holds the ISA's 64223 Cybersecurity Specialist certification. He teaches industrial control systems and cybersecurity courses in the graduate program at Wilmington University.

Sweigart joined ACE two years ago to enhance their cybersecurity and MES capabilities.

JODY WILSON

Network & Operations Manager
Delaware Health Information Network

Jody Wilson is at the epicenter of DHIN's information technology infrastructure. He oversees the production, certification and testing of all DHIN technology services, including the delivery of millions of medical results to more than 500 hospitals, practices and payers across six states and the District of Columbia.

Wilson recently led the implementation of technology to support two federal grants totaling $3.3 million to improve health IT for Delaware providers and consumers. Additionally, he manages DHIN's security protocols and disaster recovery efforts.

A Delaware native, Wison is a graduate of Smyrna High School and the USAF Technical School at Keesler Air Force Base in Biloxi, Mississippi.

Jim Garrity: It can be a lot more expensive when you're bolting in technology after the fact to try to protect yourself versus as part of your process building security into the applications you build and into the systems that you create in a way that isn't super expensive and doesn't draw against your profits.

James Collins: What are the major elements of a plan that I should have as a business to protect my business?

James DeHoniesto: Education. We talked a lot initially about information. I think you have got to understand your environment. We don't do a good enough job of educating employees of their role in the cybersecurity game.
There are certain guidelines you have to follow, but most companies are not taking the time to educate their employees on small things like phishing attacks, or not to click on things in email that could compromise your company. How do you ensure that you don't pick a password that you have to write down on 38 Post-It notes and leave on your monitor so everyone coming by can figure out your password? How do you ensure you pick a different password for the multiple systems you have so that if one system is cracked, you're not giving someone access to everything?

Scott Plichta: So don't answer the phone and give your password to the tech.


Dick Sweigart

Dirk Sweigart: We have the folks in the control-systems world interfacing with the IT people and in some cases they're the same people. Because information technology and the proliferation of Windows and so forth is working its way down into the control systems, there's an expectation by the plant managers and by the CEOs that whatever happening on my factory floor -- I can now see it because I can do it at my house. I can see what my refrigerator temperature is or I can start my car.
They expect to see that kind of data. We used to have two groups -- IT people who handled the business side of things, and process-control people who handled the process-control side of things. We can't afford that anymore. It's all converging together. That's one of the things I teach at Wilmington University. I'm teaching IT people about industrial control systems. We also need to teach industrial process-control professionals about IT systems and how to be the same people in some cases.

Scott Plichta: If you want to get everyone's attention and help them understand how to protect business assets and customer data, go through a mock exercise. You need a plan. You don't want to be caught in a situation where you don't know how to react, and you make every mistake in the book, and then your brand really suffers. When I see those breach notifications in the news, I look at how the company reacted. Mock exercises should be a routine practice for all the highest- ranking executives in a company, including human resources, legal, and marketing or public relations departments.

Everyone needs to get past the "this could never happen to us" and realize, "oh, my gosh, that really could happen; that's a reasonable scenario." So going through that process is essential because that makes you identify what your threats are. But, secondly, that might give a medium-size business the ability to put some budget behind it to prevent it from happening. So it could create awareness that there is a real threat. Then, the possibility of these real threats has to be communicated to employees regularly to remind people to be vigilant and suspicious in a healthy way.
Jim Garrity: I think everybody, and especially security leaders -- you all need advisers. Like I need advisers. Get people around you that don't think like you that are looking at some other angles in your business. Even as a strategist, you have operational thugs that are kind of doing -- it's hard to kind of elevate yourself up to look at all the angles to see where are there different, new pockets of security issues that you're not considering. I think that's really -- I think that's a key thing.

James Collins: How can a business recover from a threat or attack?

James DeHoniesto: Disaster recovery plan. We talked about education. No matter what you do, if someone really wants to get to you, they can. The best thing you can do is work through a disaster-recovery plan. And manufacturing companies and healthcare companies have done this forever -- they've come up with a plan.
What does it mean if the internet goes down? How do you do business? Do you need to have the next day's orders if you're a scheduling company? Do you have to have that printed out just in case something happens?

Dirk Sweigart: And size doesn't matter. Everybody from your hairdresser on up to a multi-national organization should be thinking about what happens if you have an incident.

Jim Garrity

Jim Garrity: It's an interesting start because what the Cloud has done is taken away one of the biggest issues on the IT side, which is that we focus on the perimeter only, on security from a network and systems perspective. That's only one piece of it.
Obviously, you have to work with your Cloud provider to make sure you've done the right things around security and information, but it limits a little bit of your risk.

Jody Wilson: I also think when we talk about moving it to the Cloud, it's really change the perception. It's a change in who's now responsible for the problem. Because you moved your hardware, your software and it is now offsite, it's all hosted -- hardware hosted, software hosted. So it really speaks to your service-level agreement with your vendor. From a public-facing perspective, the question is who is responsible for it. Is it the company that you're doing business with or is it the company you partnered with in the Cloud? You are trusting this organization to have the proper policies, procedures, and disaster-recovery plan, and that doesn't change just because you're in the Cloud.

Jim Garrity: Your hardware and software is no longer in the building. It just means it's somewhere in the Cloud, which is very interesting to the public because the general public doesn't know what the Cloud is, they don't know where it's at, they have never seen it. To them, they're still doing business with the State, they're still doing business with the hospital. So to them they don't really care where it's hosted. It's really just for an organization, especially your small and medium business organizations…now it's a transfer of ownership and responsibility.

James Collins: Say my business is not IT, but I have a lot of IT in my business. Do I need to spend up on IT?

Scott Plichta: Somewhere you have to find that partner. You can't hand over responsibility. You still have responsibility for your customer data, security, control, and your design. That is still your responsibility.

Jody Wilson

Jody Wilson: From the healthcare perspective in Delaware and from within, we recently became one of only a few Health Information Exchanges (HIE) in the country to be HITRUST-certified. From a HITRUST certification perspective, it wasn't so much about protecting the hardware and the software and the data internally, but it was more about the policies and the procedures, the education of the people, and documenting and showing what we're doing. And any organization out there, I know large hospitals in Delaware and other organizations that are going through this process right now, they have reached out to us and said, what did you guys do, how did you do it.
One thing you really have to take a look at about the Cloud is it is not so much about where it's hosted, it's the policies, procedures, and how you're going to handle it. It's the agreements that you put in place and what you're going to do. As an organization, you have to be ready to back it up. You can't just put a check in the box. You can't put it on a piece of paper. You physically have to make it part of your workflow and you have to train your employees so that they understand that it is critical, that maybe as a business it's not coming to work 8:00 to 5:00 every day. Someone that's utilizing your services out there in the community somewhere is depending on you to do a good job.

James Collins: Recently, the National Institute For Standards and Technology changed direction on passwords. Do you agree with the new thinking of making them a phrase?

Jim Garrity: I do. The next piece of advice is to stop thinking in the sense of letter-number combinations. If I wanted to use the word "house" as my password, maybe I'll change it to capital H and number zero. What you want is a long enough password -- like 15 characters or more -- that you can't …easily crack. Write a long, non-compound sentence. Jim went to the store to go buy bread. If you want to substitute numbers and letters just to add some complexity, it's fine. Is it necessary? No.

Jody Wilson, Jim Garrity, Secretary James Collins, Dirk Sweigart, Scott Plichta and James DeHoniesto attend the roundtable discussion focused on cybersecurity. The industry roundtable is one in a series sponsored by the Delaware Business Times.

PHOTOS BY RON DUBICK

James DeHoniesto: A password policy is most critical. You have to come up with something that's user-friendly. Where possible, utilize technology. Look at the same sign-on where you can or a single sign-on where that's possible so that you have one password that with two-factor authentication allows you to get into more systems. So you either use that same password or that password gives you access to other systems.

James Collins: What are the security risks that you are most concerned about and what is the antidote to those risks?

Jody Wilson: The biggest risk I see is people. It's as simple as the fact that yesterday I pulled into the office and I took a picture of an open window. An open window at 8:00 a.m. in the morning. How do we fix it? We have to educate them. Not only do we have to educate people and train them, but we have to reinforce that on a regular basis. You have to have very tight policies and procedures. They're only going to work if you're going to enforce them. You have to make sure that your employees know you're going to take this very seriously and after "X" number of violations of the security policy, they're going to be looking for employment somewhere else.

James DeHoniesto: It's the people. It's the biggest risk of every location. It's been proven time and time again. The last number in one of the surveys said that over 80 percent of the breaches were by internal fault. And it wasn't necessarily nefarious. It was someone doing something by mistake like taking a USB out of the facility with patient records on it and losing it. I think the antidote is education, convincing people why it's important, then holding people accountable to it. I know companies that have a password policy in place for everyone but the CEO because it's too hard for him. Everyone has to do it or no one does it.

"I think there are a number of organizations that believe they're too small or too specialized and they don't have to worry about this risk. Their belief is, "Not me, I don't have enough money, who wants my data, I'm just making screws and widgets, so what's the big deal? "

– James DeHoniesto

Scott Plichta: It's people. We educate and we test, but it's the same people that click the links every time, so we educate them and educate some more. I think it's up to us to put the technology and the tools in place to help, because someone's always going to click that link.

Dirk Sweigart: I worry about specific people -- people that are malicious. And they could be a disgruntled ex-employee who's mad. I worry about the hacktivists, people that think it's a good idea to cause those things to happen. The other people I worry about are the people who are complacent, that think this isn't real. They're trusting people. We need education, vigilance, and we need to put systems in place.

Jim Garrity: I think it's the unaware person most of the time who creates the biggest risk. The antidote is "process." As part of standard operating procedures and systems, I can build a model that includes training and things we can do systemically to ensure that we're living up to that policy. ■

THANK YOU TO OUR PARTICIPANTS