SPONSORED CONTENT

CYBERSECURITY

THOUGHT LEADER FORUM

Cybersecurity is no longer just an IT concern, it is a business concern.

Cyber attacks can disrupt and cause considerable financial and reputational damage to even the most resilient organization.

As businesses are more digitized, they are more exposed to an increasing number of threats if they do not manage the risk of security properly. Due to the complexity of global supply chains, pinpointing and avoiding cyber-related risks is nearly impossible. Fortunately, technologies available to businesses for cybersecurity are adapting and so is the importance of utilizing the technologies to address it.

Thought Leaders David Fehrer, CIO at Unitus Community Credit Union; Siva Narendra, CEO of Tyfone Inc.; Justin Hayden, president of Securus Systems; Tim Deggendorfer, commercial team lead at The Partners Group; and Brian Sniffen, partner at Miller Nash Graham & Dunn sat down with the Portland Business Journal to talk about the key risks and what businesses can do to prevent them. The discussion was moderated by Erica Heartquist.

Erica Heartquist: What is "cyber liability?"

Tim Deggendorfer (The Partners Group): The mainstream view is it's something that has to do with anything related to the internet. In reality, it's anything having to do with the protection and security of private information in addition to protection of your systems, other people's systems, protection from wire fraud, theft, theft via electronic means, social engineering and phishing.

Justin Hayden (Securus Systems): From a cybersecurity IT firm standpoint, it's what you're liable for within your organization. It's the pain points and risk factors that your organization has, such as banking data, Protected Health Information (PHI) or Electronic Protected Health Information (EPHI). Liability extends to the storage, access, protection and use of that information.

Siva Narendra (Tyfone Inc.): Before we talk about cyber liability, let us address the cyber space and liability of using it separately. The challenge in the current ecosystem is that the information in cyberspace is almost always controlled by one entity and the liability of the information is often with a different entity, whether it's your files in Dropbox or your personal information with Equifax. You have limited control, yet ultimately have the liability. There's a clear distinction, unfortunately, that the control and the liability ownerships are not in the same place. Let us look at another example — Apple Pay. Apple controls the device that store the payment information, but the banks take the liability. I can just go down the list. So that's a foundational problem. It's a fundamentally broken system that obviously needs to be rebuilt before cyber liability is meaningful. But the question is: do we reboot it from scratch or do we do a patchwork? That remains to be seen.

Heartquist: How much does a data breach cost?

Brian Sniffen (Miller Nash Graham & Dunn): There are studies that give a specific dollar figure per record, but for many small- and medium-sized businesses it's oftentimes not a matter of what it costs per record; if some six-figure amount of money went out of the company because they were tricked into wiring money to the wrong party, what does it cost? It's everything. They can't necessarily recover from it. Or if they mistakenly send out all of their employees' W-2 information to somebody that made it look like they were asking on behalf of the company — they made an email look like it was coming from your CFO and so you've sent the W-2 information to them — then the client has lost a significant amount of trust from its employees. The other thing is that when an incident happens, the process of investigating it and remediating it takes away the ability of people to do their typical jobs because this is generally not something that people do on a day-to-day basis. That has a significant impact in terms of revenue growth because these people can't be out selling or servicing clients. I think those costs for companies in Oregon, and the vast majority of companies in Oregon are small business, I think those are the costs that are more relevant than "X dollars per record." You may not ever recover from it because of the loss of trust, or you don't have the capacity to withstand a hit like that.

David Fehrer (Unitus): A loss of trust and really what it does to your brand. I think you can't really measure that but it certainly is difficult to recover from and rebuild trust. Certainly the hard costs can be very high and brand damage hard to measure, but it is also the cost to our members' well-being as they have to navigate through a process of protecting their identity and their money.

Sniffen: I'm a trademark attorney as well and brand is everything for a trademark attorney. We haven't really seen a long-term impact on company brands yet. So, like Target, they definitely took a hit but they're doing fine now. Other major brands like Sony that have suffered security incidents, it's hard to quantify the hit to brand value because they've all more than recovered, but that's not to say they couldn't be even further along had this not happened and had there not been a setback. I think that's really difficult because one of the main motivators from a board perspective is going to be, "What is the value that the brand is going to take a hit for?" And I don't think it's easy to determine because a lot of companies do recover.

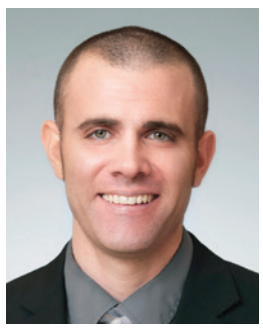
Hayden: To echo what Brian mentioned, as we navigate this new landscape of cybersecurity and data breaches, brands are going to take more and more of a hit, especially when the burden and loss are shared by third-party vendors and the consumer public. Uber and Equifax are great examples because their recent cybersecurity failures should have been an unrecoverable loss to their brand, but to borrow a phrase, "they were too big to fail." However, with increased frequency and magnitude of data breaches, companies will be faced with greater risk and accountability, and this will ultimately change how brands survive.

Sniffen: I think what we've seen is that companies that are not transparent in what happened — or come out with a statement that says one thing and then two weeks later or a month later, the statement says another thing — that's really damaging. I think folks appreciate that things happen, no defense is perfect, and the damage to brand is more an issue of covering up or getting things wrong. When we have clients that suffer incidents, a lot of times the client's first reaction is, understandably, the desire to run out and tell people what happened and "here's what we're doing." But we often counsel them to pump the brakes a little bit because in the first few days, hours, et cetera of an incident, it's really tough to determine

CONTINUED ON PAGE 31

SPONSORED CONTENT

THOUGHT LEADER FORUM: CYBERSECURITY



DAVID FEHRER

CIO, UNITUS COMMUNITY CREDIT UNION

David is responsible for the long-term strategic direction and implementation of technology. Prior to joining Unitus, David spent 11 years working at Xerox in the information technology field holding executive global positions that span financial, telecommunications, health care and retail industries. David has more than 18 years of experience in varying roles in the technology arena that includes working at ING Direct. He has successfully launched multiple data centers, call centers and innovative technology solutions that encompassed a multitude of technology platforms and customers. David holds a Bachelor of Science in Computer Information Systems and an MBA from Saint Leo University.

SIVA NARENDRA

CEO, TYFONE INC.

Siva is co-founder and CEO of Tyfone Inc. Before his current responsibility, he was with Intel Laboratories specializing in energy and yield aware designs. He has authored over 60 technical papers in peer reviewed conferences and journals, and frequently lectures on technology forums. He also has over 300 issued/pending patents and holds 5 divisional recognition awards from Intel and an award in 2003 for having 19 issued patents in that year. Siva has a Ph.D. in Electrical Engineering from Massachusetts Institute of Technology. Siva is located in Portland.

JUSTIN HAYDEN

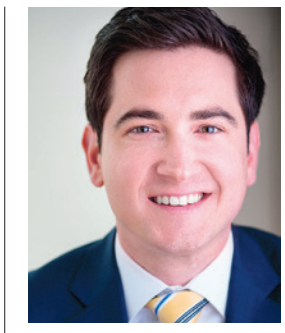
PRESIDENT, SECURUS SYSTEMS

In 2010, Justin Hayden founded Securus Systems as a full-service information technology firm providing comprehensive support to small businesses. Soon thereafter, geopolitical instability gave way to increased cybercrime, and Hayden seized the opportunity to offer cybersecurity services. This change in direction was pivotal for the company, and Securus became a welcome resource to an underserved market. As cybercrime became an increasing threat to businesses across all industries, Securus grew its reputation as the West Coast leader in cybersecurity. Under Hayden's leadership, Securus Systems has grown into a multimillion-dollar firm with clients ranging from health care and professional enterprises to local and regional businesses.

TIM DEGGENDORFER

COMMERCIAL TEAM LEAD, THE PARTNERS GROUP

Tim brings extensive industry knowledge after 20 years of experience in sales and account management. In his role at TPG, Tim focuses on developing commercial business organically and integrating current clients into TPG's suite of commercial services. He is also responsible for identifying new producers to grow the Portland Commercial Insurance team. Tim has a B.S. in Economics from Lewis and Clark College and is a Certified Insurance Counselor.



BRIAN SNIFFEN

PARTNER, MILLER NASH GRAHAM & DUNN

Brian Sniffen, a partner with the law firm Miller Nash Graham & Dunn, helps clients manage and enforce intellectual property rights and assists clients with the data-security aspects of their business. He regularly advises on trademark and copyright issues, such as fair use and infringement, and is skilled at getting infringing content removed from the internet. Brian evaluates clients' data-security practices and the applicability of various laws, regulations, and rules, helps draft privacy policies and data-security policies, negotiates vendor agreements (e.g., SaaS, PaaS, network services), and responds to data-security incidents. Brian can be reached at 503-205-2443 or at brian.sniffen@millernash.com.

CONTINUED FROM PAGE 29

what happened and we don't want to come out with a statement that says, "This is what happened and this is what we're doing" and then a few days or a week later say, "Actually..." and have to backtrack. That can cause as big hit as far as trust goes.

Fehrer: I do think that's where it's important for companies to utilize attorneys and professional resources because this isn't something that most companies do on a daily basis; actually talking about a breach. So they do want to have transparency within themselves and to the customers. But a lot of times that transparency can cost them because they come out with too much, too early before they actually have all the right information. I think having the right people engaged and taking a step back can help with the right response and maintain trust.

Narendra: Data breach has an impact on brand reputation which, in theory, could be catastrophic. To talk about brand reputation and we have to talk about brand experience. If you ask a consumer, they're not worried about your brand reputation. That's your problem. They're more worried about brand experience. That's where every digital solution that gets into cyber space by a service provider, be it a financial institution or Amazon, they're focused on providing a rich brand experience. Security is often an afterthought. And that's because, traditionally speaking, security is a trade-off for convenience. Therefore brand experience is a trade-off for brand reputation. So a service provider has to pick and brand experience wins every time. That's the problem. You need to foundationally build the system keeping security in mind. There is a novel thought, "If one can actually make your digital life secure by decentralizing security, it can be really convenient." You don't have to remember passwords, you don't have to remember all answers to intricate questions, that we enforce down on consumers. Without frictionless security, it is a beautiful experience except one has to live with crappy on-boarding, login and password resetting processes. With frictionless security we can certainly minimize the brand reputation cost due to breaches while preserving brand experience.

Sniffen: And consumers demand these technological systems for free or very low cost and shop these systems based on cost without ever having looked at the terms and conditions or what the contract with the vendor actually says. We have to say that security does cost more and it's not enough to just have a flashy brand if they're not good custodians of your data.

Narendra: Published data, I don't know, about a year ago said four percent of the cyber security budget is spent, not for individual institutions, just generally. Four percent of the cyber security budget is spent in preventing digital identity loss. Ninety-six percent is spent in curing it up. That's because foundationally, we all think "experience." We want to make the experience really beautiful, which is important. But if you build it right, security and experience are the same thing.

Deggendorfer: I think part of the problem is that cyber liability is so new that people don't understand it and they think it's just the hacking of private information. You can quantify what it's going to cost per record on a data breech. Is it $200, $300 per year to notify and monitor? But it's infinitely more difficult to quantify other areas of cyber liability. You've got the intangibles, the brand reputation. You've got the monetary fines and penalties from governmental agencies and that's going to vary depending on the industry, loss of income to the actual client. Extortion? Have the servers been hacked and held hostage? There are so many different variables involved, and it's still such a new product and new space, that there's not a lot of actuarial information out there to put some real quantifiable numbers to a lot of this.

Hayden: Exactly. There are some sobering facts like the average cost of a data breach in the U.S. is $1.3 million for enterprises, and $117,000 for small- to medium-sized business, and of those attacked, 60 percent go under. Why? Time. The average time to resolve a malicious insider attack is 50 days, and the average time to resolve a ransomware attack is 23 days. Then the cost becomes a question of how much data was lost? The data recovery, incident response and mitigation are additional expenses to the days a business can't function normally. Long-term costs should also be considered. If a medical facility is attacked, the initial cost of a data breach doesn't include when OCR (Office for Civil Rights) is coming in and auditing for HIPPA (Health Insurance Portability and Accountability Act) violations two years later. The violation fines are staggering and all because a business didn't take a proactive, offensive approach. Health care is a favorite target — in fact, it's the number one industry attacked — because medical data contains everything from financial information to Social Security numbers and employment history. Four out 5 U.S. physicians have experienced a cybersecurity attack, and victims of medical identity theft spend an outrageous average of $13,500 to restore their records. Again, the cost of a data breach cannot be isolated. It's far-reaching.

Deggendorfer: A lot of companies, especially the larger ones, are going to play the law of large numbers. "We're going to pay it just a little attention, slap some security on there and take our chances," because they don't want the customer's experience to be impacted.

Heartquist: When discussing cybersecurity, what are the hardest channels to secure and what are some of the best tactics to secure them?

Hayden: The number one cause for any cybersecurity attack is the human element. It's the number one. It's consistent education and training. For their IT needs, a business typically wants security, speed and quality all within a cheap budget. You can't get all three. You can't get something quick and cheap and expect quality as well. So Securus Systems tries to find balance, and the most effective, most broad security solution is to train employees.

Fehrer: I agree. That's exactly where I'd go too. Anytime that you have a human interaction, that is the hardest area. Really all you can do is build the right information security program and make sure that you have the right controls in place, your checks and balances. You're testing it continually and then you're doing the right level of training with your employees. There's only so much you can do but that's absolutely, I think, the right path to walk down when you're trying to secure those channels. Those are certainly the hardest ones but the most valuable if you get it right.

Hayden: We can lock down everything in terms of network and bank structure, but that doesn't matter if an employee compromises those measures. If an employee hands out their password or loses their work phone, then there's only so much we can mitigate after the fact. It's vital to prevent those mistakes from happening in the first place.

Fehrer: A lot of companies, I think, do miss the training portion of it or they don't focus heavily enough on the education to their employees. Sometimes even to their customers or members.

Hayden: And most small- to medium-sized businesses think, "It's not going to happen to me. It happens to the JP Morgans. It happens to the Ubers. It happens to the bigger guys. It happens to the CEO or the CFO. They're not coming for me." But that's a false assumption and a dangerous gamble. Forty percent of all cyberattacks are focused on companies with less than 500 employees.

Deggendorfer: A lot of people also have the misconception that, "Well, I'm not holding the information. I'm not retaining it. It's going to the payment card provider." A lot of people use a third party to maintain their systems outside of IT and trying to get them to understand that, "You were the source of the information. It's your problem," can be hard. Education becomes huge. From a cost standpoint, I don't think there are any barriers. Premiums have come down significantly in the last few years and you can get in from a baseline product very reasonably no matter what industry you are, regardless of what your security systems are. Carriers will accept very, very basic lockdowns on your system. It's crazy what they will accept to insure somebody. So cost from a tangible standpoint, I don't think is a barrier any longer. It's just primarily education.

Narendra: Human element is the hardest cyber security problem to solve. But we're living in a world where we're going to have self-driving cars with no human element involved. You can't have cyber security have this human element involved because it is unsolvable for the following reasons: humans use passwords as our primary security and we can't double our password length every 18 months since computers have become fast enough to compromise the passwords. Twenty-years ago that wasn't the case. Computer speed were much slower and password complexity was high enough for it. Password complexity has nominally increased over time, and computer speed has significantly increased and doubles almost every 18 months, as predicted by Gordon Moore. We can't double our password every 18 months, no matter how much training we do. So we just have to look at it as, "How do we solve the fundamental problem?" You can't encrypt the data, put the decryption digital keys right next to it and protect it with a tiny password. Take the keys and put them in your pocket just like your chip card in payments. Let's use a decentralized technology where your information cannot be cloned. Let's not introduce a human element. You have to train the human to do something different, like insert the card when you're at the point of sale and press a button on the card to log in remotely. Relying on human element is unsolvable. This is going to be really important especially as we look at blockchain and decentralized ledgers.

Sniffen: And what we often see is so simple. It's an email coming in to somebody, a well-meaning employee, it's very rarely a nefarious insider, and the well-meaning employee is being asked to do something and they either don't call the CFO or somebody else to verify that, "Yes, this wire transfer is supposed to go out" or "Are you sure you need all of this W-2 information?" It's really basic stuff and then I think what you're eluding to Siva is some sort of multi-factor authentication where you have something with you physically that is a second step so that when you go to log in on something, you actually have to have a passcode or a key card or your phone with you to say, "Yes, that is me logging in," and that would solve so many of these really basic problems.

Narendra: I always say, "I drank my Kool-Aid, so my tongue is purple." With that disclaimer, I want to mention eliminating human element for securing cyber access needs the solution to be cryptographic so we can digitally lock the information. Which means we have cryptography keys to do that. If we using a phone for it, the question is, "How do the keys get into the phone in the first place?" It cannot be by typing my password. Password as a weak link cannot protect cryptographic method that is a strong link. Identity issuers don't make the phone, but in every case they can issue smartcard chip cards. So you can be proofed by the issuer and given a card with keys in it. By making the cards work in cyberspace through wirelessly connecting it to devices you not only have it multi-factor but decentralized and unclonable. Yes, this will require user behavior change, just like use of chip cards at the point-of-sale did.

Deggendorfer: But as we've all said, it's got to be easy enough to use, and people have to be willing to use it.

Narendra: That's right. And the chip card took 20 years, global planning implementation standards, training the users that you don't have to sign in. It takes time because you're requiring consumer behavior to change. And it's coming.

Heartquist: The old saying goes practice makes perfect. Is it possible to apply that within cybersecurity?

Fehrer: Certainly for us and what I've seen as well, practice is very important and I think how you practice is to test it. That is, working with third parties to come in and test your controls, test and look at your employee's behavior. You take that feedback and use it to help close the gaps and see where the areas of opportunity are. As we're saying, there's a lot of technology that has been coming along, but that human element will always be a factor and so the more you test and train, the stronger you can make your program.

Deggendorfer: It's never going to be perfect because technology is so rapidly changing. Continuous training and continuous improvement on system and employee training is going to be vital. Companies that aren't going to do that are going to suffer.

Fehrer: It's kind of an iterative process. I mean, you're always changing it. There are always new threats and you've got to stay on top of it. You can't just sit back and say "we've got this covered," because that's when I think people get into trouble.

Narendra: Another reason why practice and training are pretty critical is there are so many interdependencies, right? Ask Target. You may have the perfect system but there is no short circuit to practicing the use of it. Not just you, but also your direct vendors.

CONTINUED ON PAGE 32

CONTINUED FROM PAGE 31

Heartquist: What advice would you give me if I were the owner of a small business through training first and foremost?

Hayden: Constantly train your employees. Typically, an organization won't go beyond new employee onboarding and training. So many businesses stop after an employee is trained on their systems and job expectation, and that's the Achilles' heel in terms of cybersecurity. So the best preventative action is to continue education on changing systems and new threats. Building awareness is key, especially as threats become more and more sophisticated. It's no longer the wiring money email scams. Cyberattacks are becoming complex and personalized, and even the most knowledgeable, most responsible employee could be duped. Employees need to be trained to ask critical questions and keep an ongoing dialogue about what to expect and how to react. Otherwise, it's "out of sight, out of mind."

Fehrer: I think the testing and the training needs to be continuous, but the adjustments to it and fresh looks and updating it based off of the newer threats and technologies is also really important. If you create this continuous training that ends up being stale and ends up sitting there for four or five years, you're so far out of date that you're missing most of the new threats.

Deggendorfer: It's a multi-faceted approach. You have to have the security systems on your IT as well as training your employees. Even then, nothing is fool proof. At my last company, we had a training for all our staff and everyone was in attendance, but one employee. The very next week, she was the employee that got an email asking several phishing questions. Luckily, she asked for guidance. But what are the odds that out of two dozen employees she would be the one that would get it? Even with training no system is perfect.

Hayden: As a cybersecurity IT firm, we'll constantly test clients' employees. We'll send out tests on the newest technologies or phishing techniques, and the aim is to identify vulnerabilities within an organization's workforce. Employees who show risky IT behavior are required to go through additional training, or if there's a widespread trend, we make recommendations to management about the organization's overall infrastructure. We maintain logs to show progress and improvement because, again, cybersecurity is a constantly moving target. Then if there is a cyberattack, we can quickly identify and investigate probable sources, saving both time and money.

Fehrer: And in terms of when we do have one that sneaks in sometimes, an actual true phishing, we've got a place to send it. We validate it and it's been very effective doing what Justin just walked though. Sending these test emails and then we go back and see who failed and clicked a link, then provide that additional training. Having an information security program is also important, the right systems, the right processes and procedures documented so that everyone can understand it and it's built into the training, and then validating and testing those controls. With a small business it's a little bit harder, you don't quite have some of the same funds that the larger corporations have, but there are still the basics. Cover the basics and make sure you're incorporating that into what you're doing on a day-to-day basis.

Sniffen: I think part of what you're alluding to is what we call an incident response plan. That's one of the things that has been shown to reduce the cost of data security incidents. With an incident response plan, when something happens, you already have a plan and steps to follow. It's generally written and kept with executive level materials. And it doesn't have to be complicated. It can be just really basic stuff like how you're going to go about investigating and remediating, and what are the steps you're going to take to investigate, who's on the team, who can you call with numbers and contact information included. That may include your insurer. It may include your lawyer. It may include law enforcement. It's often an iterative process that feeds back on itself.

Fehrer: That's absolutely part of it. I think it can go even beyond that to "How do you manage your passwords, how do you manage your accounts? How are you logging in? How are you looking at the logs?" There's a lot, I think, to it but certainly, incident response is a very big piece that I think a lot of people miss.

Deggendorfer: As part of that incident response, if you have a cyber policy, every one of them is going to have a third party vendor that you can use as a first point of contact that will have initial incident response. They can help start to diagnose the problem and they've got public relations people that can give you advice and get out in front of any potential bad publicity, if necessary. If the problem requires it, the carriers will send public relations professionals with boots on the ground to help you manage the crisis, whether it's the news or clients; there are all kinds of resources that are part of your policy that are included and are free.

Narendra: The interesting thing if you look at the various points that we're making, we have to be correct every single time; a criminal has to be lucky once. That's because we've put all of our assets in a centralized place, not physically centralized, but logically centralized. That's like defending a digital fortress with all the soldiers on the inside. That requires human element training unless and until we decentralize security which is going to take time. Meanwhile we do have to figure out, "How do we manage this?" And what I usually tell our customers is, "What's the worst that could happen?" The question is very unique to each industry and each institution. The DOW Jones Industrial Average tells us how the market is doing, but we don't have a way of measuring cyber security risk. How can you improve something that you can't measure? So this training piece and the management team for each institution needs to sit down and say, "Okay, let's think through. If everything went wrong, what's the worst that could happen?" From a brand reputation standpoint, it's difficult to compute, but you can certainly look at the monetary risk and then you can plan around it.

Heartquist: What groups or organizations are most vulnerable to cybercrime, and who is responsible for these attacks?

Narendra: I don't know if you've gone to the dark web to see what kind of service level these cyber criminals provide, things like $200 in bitcoin guarantees a compromise. That's the organized part of it. Who is vulnerable? Everybody. Equifax data loss is making this worse because that is the information service providers in cyber space ask, to know who you are.

If any of you have tried to freeze your account by calling Equifax and all these credit bureaus, the information that they ask to freeze in your account is what they lost. By the way, if you haven't done it, please try it. It's all touchtone based. How long do you think it's going to take to automate that? Cybercrime is going to be a $6 trillion industry by 2021. It's bigger than, really, a big chunk of industries on the planet. The cloud service has commoditized data and transactions so I don't think you can rest easy saying, "Oh, it's not going to be me."

Hayden: And that's just it, the cloud services have made things easier and more accessible for all businesses of all sizes, but it goes back to a fallible assumption. People wrongly assume that because they're using a brand name cloud product like Amazon or Dropbox, then they're secure and that the regulatory compliance isn't their direct responsibility. Let me be clear, that's simply not true. There is shared liability, and shared consequence. Again, look at the Equifax breach. The cloud can be compromised at the server level, and it doesn't take an insider or hacked password. It takes time and someone with just enough information to be dangerous.

Sniffen: The majority of businesses that are impacted by data security incidents are small businesses with 1,000 employees or less.

Heartquist: Then how do organizations defend against cybercrime?

Hayden: From a cybersecurity IT firm standpoint, there's not just one area. It's not a checklist like, "You go and buy this service, or you go get that product, and do this one thing for the best defense." If an organization is serious about protecting its future, they need everybody in this room. You need legal counsel, a cybersecurity strategy, an insurance policy and business partners with the same attitude and approach. But that's just the preventative side of this coin. The other side is when a breach inevitably happens, because it will happen. An organization must be prepared with both a proactive and reactive plan. How hard is it going to hit you? Reduce that unknown by utilizing the necessary resources and expertise.

Fehrer: It is about the entire thing, right? Looking at your practices, your policies, your procedures. Really, all the mitigating controls you have in place, the right systems, which you're monitoring. You're doing the alert and making sure you have all of that aligned and you're continually testing and then you're continually training and reiterating on that throughout the process. I think those are core and key. For us within Unitus, it's important to take that member lens too and make sure we're looking at our members as that is the core of what we do. It's not just learning for us, but also, "How can we help them to potentially guide them to avoid some pitfalls?"

Deggendorfer: It's got to be viewed from the top as being important and vital to business. If it's not, it's just going to be like anything else, there's going to be no value in it. It has to be prioritized and it's got to be a global approach. There is a lot more to it than just buying an insurance policy, it's the total component.

Hayden: I think we need to see a shift in the attitude and approach to cybersecurity IT and its value and role within organizations. There is still this divide between cybersecurity IT as a service versus an integral part of the business. It's an ignorant and outdated approach because cybersecurity IT has evolved beyond simple software and helpdesks and new tech. Cybersecurity IT is an essential function of a business, especially as we rely more on the Internet of Things (IoT), or how devices and systems are connected. There are some businesses that get it. A Chief Information Officer (CIO) really deserves a seat at the table with the CEO and CFO because cybersecurity IT is a pillar of the organization.

Sniffen: I think that will start to change because of lawsuits. Shareholder derivative lawsuits and all sorts of litigation are taking aim at corporate directors and officers in the wake of data breaches now. So far, there hasn't been a lot of success with these claims but that hasn't stopped them from being filed. And corporate officers and directors who have prevailed did so because they meaningfully addressed cyber risk — like in the Wyndham (Worldwide Corp.) case. The board regularly discussed cyber security issues. Yes, they suffered a breach but they meaningfully addressed it, discussed it at a high level and took steps to remediate where they knew that they had problems. I think companies that don't do that are making themselves much more vulnerable to such claims. But on the topic of what organizations can do to defend, Oregon is made up of so many mom-and-pop small businesses. I think a lot of people are just so overwhelmed by the potential expense and the resources that it's going to take. But there's so much basic stuff that they can do. I think just starting. Starting the process is going to be a monumental step in the right direction.

Narendra: Organizations can do two things. First, acknowledge that while security is not a sexy thing to talk about, you have to. It's sort of like exercise. We all know we have to do it consciously and dedicate time, but most of us don't. I think each individual institution can sit down and figure out, "What are my risks? What is the worst-case scenario? How am I going to measure it?" Then you can figure out a way to improve it. Second, recognize that cyber criminals are tremendously collaborative with each other. Generally speaking, we're fighting an army that's very well organized and we're not. We're making their lives easier for them. It's easy for us to organize to prevent the problem. It is a collective effort, but it's doable.

For more information on Thought Leader Forums:

Contact **Anne Van Gordon** at **503-219-3406** or **avangordon@bizjournals.com.**
Future topics include workforce development, succession planning and higher education.