TABLE *of* EXPERTS

EVER-CHANGING THREATS

Ransomware, rising cyber-liability insurance premiums and remote workers keeping organizations on edge

SPONSORS

GODFREY & KAHN S.C.

ISCORP™ MANAGED SECURE PRIVATE CLOUD

University of Wisconsin Whitewater

Moderator

KATHY HENRICH

CEO
MKE Tech Hub Coalition

Kathy Henrich is the CEO of MKE Tech Hub Coalition, a non-profit focused on inclusively doubling tech talent in the Milwaukee region. Together, our 125 member organizations help build long term economic prosperity and create life changing opportunities! Kathy has over 30 years in the tech industry, including leading sales, partnerships, and consulting organizations.

Cybersecurity is becoming increasingly complex. Remote workers, interconnected supplier and customer networks, and ever more sophisticated phishing attacks are keeping cybersecurity professionals up at night – even as cyber-liability insurance premiums rise. Finding solutions that protect a company's data without interfering with productivity requires a strategic framework that encompasses the corporate culture, workflow and product development, as well as customer and vendor relations. In order to get an idea of the new cybersecurity landscape, the Milwaukee Business Journal recently assembled a panel of experts to explore what companies – large and small – need to know about today's changing threats.

KATHY HENRICH: Cybersecurity is changing rapidly, especially with the current geopolitical situation. What cyber threats are most concerning to businesses today and how are they changing over time?

SARAH SARGENT: We've seen a lot more security instances that are caused by vendors, including software vendors. In the Kaseya ransomware incident, for example, the threat actors used the managed service provider's software to push out the ransomware to Kaseya's customers. We found a huge problem with Microsoft Exchange last year. Ransomware has become the most prevalent security issue that companies worry about. In addition, cyber criminals are getting increasingly sophisticated with their phishing emails, making them very difficult to identify.

SARA DESCHNER: Another major concern is credential breaches. People have shared or weak passwords for a lot of different things and that creates vulnerabilities across the board. If a cybercriminal can gain access through one of those passwords, maybe one for a personal email account, that vulnerability can then spread into the company network if not detected.

PATRICK BARWICK: Ransomware is probably the biggest concern, but there is an extremely wide range of exploits that companies have to watch out for. Because of that, companies really have to focus on making sure employees are aware of those potential risks. They also have to keep their systems up to date and make sure they are locked down as much as possible. One way to do that is a concept called Defense in Depth, which is a layered approach to protecting data. Think of it like an onion with your most critical data at the center. You create layers of hurdles that the bad guys have to keep peeling through so they can't get to your most important information.

The experts

PATRICK BARWICK

CISO (Chief Information Security Officer) at Integrated Systems Corp in Mequon, WI.

Patrick has been with ISCorp for nearly 20 years and has been in the IT industry for over 30 years. Patrick is both a Certified CISO and a CISSP (Certified Information Systems Security Professional). Patrick graduated with honors from The University of Wisconsin Milwaukee with a Master's of Science in Management of Information Systems.

SARA DESCHNER

Assistant Dean for University of Wisconsin-Whitewater College of Business and Economics: Wisconsin's largest AACSB-accredited business school

Promoted from instructor of Information Technology and Supply Chain management, she has been with the university since 2006. Ms. Deschner has 29+ years combined IT experience: working, teaching and consulting.

SARAH SARGENT

Attorney in the Data Privacy & Cybersecurity Practice Group of Godfrey & Kahn

Her practice focuses on assisting clients in implementing innovative technology and finding practical business solutions for privacy compliance. She advises clients on software licensing, vendor management, data breach prevention, GDPR, CCPA, SaaS and more.

HENRICH: The pandemic has not only changed the way people work, but also companies' security profiles. What do companies need to know about making sure their systems are secure when they have remote workers or workers using their own devices?

BARWICK: The corporate office may still be secure, but now you have remote workers – scattered bubbles that you have to protect. That has prompted companies to focus on endpoints – the laptops, phones and other devices employees use – because that is how hackers are gaining access. There are technologies to protect those endpoints, including mobile device management (MDM), multi-factor authentication (MFA) and VPN software that encrypts traffic between the remote bubbles and the corporate network. Using these three in concert can make your remote access very secure.

DESCHNER: When the pandemic hit, companies told everyone to work from home and they had to do it very quickly. They weren't as concerned about security as they were about keeping their businesses going. Now that the pandemic has changed the way people work, it is very important for companies to make sure they have policies and expectations in place. They need to set standards about securing home networks and about how people are going to function when they are not on the organization's physical campus. Working from home needs to be considered an extension of the office when it comes to cybersecurity.

SARGENT: I agree. The pandemic caused a lot of companies to go remote when they were not technologically ready. They have had to do a lot of shoring up after the fact in order to become secure. When the pandemic first hit, I was very busy with incidents that were caused because remote desktop protocols (RDP) had not been set up correctly. In addition, many smaller businesses were

relying on a part-time IT employee or managed service providers (MSPs) who were not as security-focused as they needed to be. Now that remote work has become more commonplace, it is very important that companies have internal policies setting expectations for employees working remotely.

HENRICH: The golden triangle of security has three important components: people, processes and technology. Talk about the things that need to be done for each to make sure there are no weak links that hackers can exploit.

BARWICK: All three components can be dealt with properly if you do a good risk analysis of your operations. Every company has engines that make it profitable and data to protect. You want to protect those high-risk areas with as many layers of defense as you can. You have to make sure you understand your workflow and then backfill it with technology that will keep it protected. And it has to be a cycle of continuous improvement because workflows and threats change.

DESCHNER: In order for a company to have a successful cybersecurity plan, it needs to be embraced and championed by the highest levels of the company. Top management needs to empower the organization to design the processes and policies that Patrick was referring to, and then those processes and policies have to be communicated to the employees through documentation and training. Employees need to understand what the risks are and have a very clear plan of action they can follow.

SARGENT: On the procedural side of the triangle, I would say there are three documents that every company should have no matter how small they are: a written information security plan, or WISP; an incident response plan; and a backup and disaster recovery plan, which is also known as a business continuity plan. These documents will be on the simpler side if your company is small, and complex if your company is large. What is important is to have them and to make sure your team has a good working knowledge of them.

HENRICH: Focusing especially on the people aspect, what is being done to increase cybersecurity awareness in employee training and school curricula?

DESCHNER: It is important for companies of all sizes to do cybersecurity awareness training, to keep employees up to date with the current scams. Your employees need to be skeptical about emails and requests for information. You need to proactively test them with phishing attempts to see if people respond. We are seeing an increase in the demand for managers to become cybersecurity-aware. There is an increased interest in cybersecurity degrees. There is also more interest in broad-based training for managers in various disciplines so that they understand how they can be proactive with cybersecurity.

BARWICK: Security concepts are what is really important because technology is always changing. If you follow the concepts, it doesn't really matter which tools you use. There are a lot of great security governance frameworks out there, including ISO 27001 and NIST. Those frameworks and concepts need to be taught and followed.

SARGENT: As Sara touched on earlier, you really need management and executive-level support. You have to create a culture of security. You can't think of security as just a firewall. You have to think about how to integrate security into all of your services and products. How is R&D thinking about security? We continue to move into the world of interconnected products – the Internet of Things – and that carries a lot of risk. The next new and greatest Bluetooth widget may be a real time saver, but is it secure? Too often, companies don't think about that until it is too late.

HENRICH: Talk a little about the importance of mitigating risk through insurance and contingency planning. What does a company want to look for in terms of insurance and what needs to be included in the contingency plan?

SARGENT: Every company should have some form of cyber-liability insurance. The amount of coverage depends on your industry, the type of data you have, the number of records and how personal the information is. I think it is very important to work with a broker knowledgeable in the cybersecurity space because insurance has gotten expensive over the last year and there are many more hoops you have to jump through to qualify for it.

BARWICK: Cyber-liability insurance is getting very expensive and requires more and more security checkboxes to be completed. Some insurers are even removing or limiting ransomware coverage. As a result, there is a renewed emphasis on prevention and contingency planning. Ransomware can cripple you, but if you have a contingency and or disaster recovery plan that will let you bring your backup data up at an alternate site, you can get back into business quickly. There are a lot of great tools out there for that automation.

DESCHNER: Contingency plans really have to be a cost-benefit analysis. There will be a slightly different model for each business. You have to take a look at your greatest vulnerabilities and what is most important for keeping your business operating. You need to know who is accessing your network, which vendors and which customers. It really comes down to understanding risks and knowing how your business operates day-to-day, and finding a plan to protect your business within your budget.

HENRICH: What about small companies? When should they start to seriously consider cyber insurance and contingency plans? And what are some "simple" steps they can take to make sure they are secure?

BARWICK: Hire subject-matter experts and MSPs to host your data. They can deploy systems with hardened templates. They can help you create the rules that will keep your network from being exposed to the entire internet. Make sure your MSPs are doing what they say they are doing with SLA agreements. Use service providers that are SOC1- and or SOC2-compliant because that means they have a mature information security program. It is impossible for most companies to know all the components of cybersecurity. Using external experts protects businesses and allows them to focus on what makes them money.

SARGENT: Turn on multi-factor authentication whenever you can. I have it on my social media accounts where possible. It is already built into the tools that a lot of small companies use, but many people choose not to turn it on.

DESCHNER: Many cybersecurity concepts originated in anti-fraud efforts – minimum permissions and multi-factor authentication, for example. These concepts have benefits that extend beyond cybersecurity. When you invest in these practices, you are doing more than just protecting yourself from a cybersecurity attack. You are also hardening your business model. Even small organizations can benefit from starting with these steps.

HENRICH: Many people envision hackers to be teenage kids or petty criminals, but it has become a big business that is not going to be going away any time soon. Can you provide any insights on this and how it impacts how businesses and educational institutions should prepare?

BARWICK: It is an extremely big business. And I don't think it will ever go away because companies continue to push out products as fast as they can. They are not really concerned about the security risks in those products until they are exposed. Only then do they release updates. Most software is built on existing libraries and tools that are archaic and can contain vulnerabilities. The Log4j is a prime example of that. It's buried deep into enterprise-level applications and was exploited extremely easily. What we have is an ecosystem that actually supports the business of hacking. We have to make the best of it and continue to do what we can in order to thrive.

SARGENT: I have been speaking regularly on cybersecurity for five or six years now, and people are surprised every time I mention that a lot of ransomware gangs and cyber criminals are backed by nation states and countries. These are very organized groups that pay salaries, focus on customer service and are concerned about their reputations and brand within their industry. When people realize that, they begin to understand the true level of the threat and the urgency needed to protect against it. And one attack can have a real impact. The Colonial Pipeline incident is a prime example. Ransomware shut down a major pipeline, creating massive fuel shortages. It is an ecosystem we are continually trying to fix, but we have not found the golden key yet.

DESCHNER: I think that ecosystem will get more complex as we become more interconnected, and the risk of breaches becomes greater and greater. Companies are connected to their vendors and their customers' systems. A cybersecurity attack on a supplier or customer can prevent you from making your product or delivering a service. Getting a fundamental understanding of the scope of the threat we are dealing with is key. As technology infiltrates every aspect of our personal and professional lives, we are constantly playing catch up. Larger companies are having trouble finding the talent they need, and smaller companies must look to external partners in order to bring the necessary scope on board. But everyone should be making the investment to ensure they have the talent to lead their company in planning and protecting.

HENRICH: If there were one thing you would want business executives to take away from this conversation, what would it be?

BARWICK: You can't do it alone, but fortunately there is help. The Cybersecurity Infrastructure Security Agency (CISA) is a phenomenal resource. Subscribe to their emails and updates. It also has a database of known exploitable vulnerabilities. Reach out to cybersecurity experts. To paraphrase Vanilla Ice: Stop. Collaborate. And listen. It really is all about taking pause, working together, re-evaluating, and communicating.

DESCHNER: Whatever you are doing now, step it up a notch. It can seem daunting and overwhelming. Nobody can do everything that needs to be done but do something. Understand where the risks are in your company and start chipping away at them. Seek out external partners for help. Ignorance is not an excuse, so everyone needs to start developing their plan.

SARGENT: Prepare for a security incident or breach. Practice with tabletop exercises where you pretend a breach happened and execute your plans. Hopefully, the breach will never happen, but if it does, the organizations that have thought through what they would do recover much more quickly. That preparation can be costly, so you need a budget behind it, and you have to have executive-level support.