BIRMINGHAM BUSINESS JOURNAL

TABLE of EXPERTS Series

Insights into CYBER SECURITY

Sponsored by:

ADVERTISING SUPPLEMENT

THE EXPERTS

Conrad Bell | Principal Enterprise IP Operations and Security Architect, C Spire

Conrad Bell has over 20 years of experience in Information Technology and Cybersecurity. Conrad's current role at C Spire as the Principal Enterprise Security Architect is to direct the Office of Cybersecurity's cross functional teams in aiding each line of business to reduce risk while delivering services. Conrad's career experience spans across a variety of leadership positions at tactical, operational, and strategic levels of both government and private sectors. From his service to our country in the US Marine Corps, to his role as Lead Technical Architect at the University of North Texas and Sr. Network Security Architect with General Dynamics, Conrad is experienced in developing policies and configurations, securing infrastructure. Conrad has a Bachelor of Science degree in Computer Science and a Master of Science degree in Information Assurance. He also holds several industry certifications, including Certified Information Systems Security Professional (CISSP) and Computer Hacking Forensic Investigator Certified Information Security Manager (CISM).

Jordon Cochran | Cyber Security Management Advisory Board, Auburn University's Harbert College of Business

Jordon Cochran serves on the Cybersecurity Management Advisory Board in the Harbert College of Business at Auburn University and is currently the Chief of Future Operations and Planning at the Joint Force Headquarters – Department of Defense Information Network, Fort Meade, Maryland. He has over 23 years' experience in the U.S. Air Force and Joint Service communications systems, networks, and cyberspace security, operations and defense. He served a year in combat in Afghanistan and supported global missions in more than 30 countries. He is an honor graduate of Auburn University Computer Engineering, 1995; a graduate of Auburn's Technology Executive Masters of Business Administration, 2003; and holds four other master's degrees, including one in Computer Systems with an Information Warfare focus.

Paul Perry | Member, Warren Averett

Paul Perry has been with the Firm since 2004 and is a Member and the practice leader of Risk and Controls in the Firm's Risk, Security and Technology division. Paul and his team focus on cybersecurity, risk assessments, industry-specific compliance, internal controls and information technology control-related projects, including Service Organizations Control engagements. Paul is also the leader of the Firm's Data Analysis Group, a team of individuals within the Firm who provide data analysis solutions to both internal and external clients. For more than 11 years, he has specialized in auditing and assurance services. Paul has extensive experience serving clients in the nonprofit, governmental, financial, insurance and healthcare facilities/hospital industries. Paul has earned the Certified Information Technology Professional (CITP) certification.

Mike Roman | Senior Risk Consultant & VP of P&C Operations, Valent Group

Mike Roman, Vice President – Property & Casualty Operations & Sr. Risk Consultant, Valent Group (An EBSCO Company)

Over the past 14 years, Fortune 1000 publicly traded and privately held companies have trusted Mike with their comprehensive risk management programs and relied on his deep technical expertise in cyber and management liability. Mike now champions these specialty practices for Alabama's small-to-midsize businesses. Mike is a member of the firm's leadership team, overseeing the daily operations of Valent Group's Property & Casualty department. Prior to his work in risk consulting, he was a pilot with American Airlines after a distinguished career as a Naval Aviator with the U.S. Navy. He has a Bachelor of Science degree in Mechanical Engineering, with distinction, from the Virginia Military Institute.

India Vincent | Partner and Chief Privacy Officer, Burr & Forman LLP

India Vincent is a Partner at Burr & Forman focusing on helping clients identify, protect and generate maximum value from their intellectual property as well as helping clients develop and implement policies and procedures to protect their data. India's areas of practice include intellectual property, technology, corporate transactions, cybersecurity and data privacy. India assists companies with identifying their key assets developing customized, situationally appropriate security and data protection policies and breach response plans. India works with clients in all industries, including the software, technology, biotechnology, entertainment, health care, hospitality, aerospace and manufacturing industries.

THE DISCUSSION

Q: What are some tangible things my company can do to reduce the risks of a cyber-attack?

Paul Perry: The major one is the security measures you have around the technology environment at your organization. Things like controls to put in place or policies to write. Another is education. Educating your employees to do the right things is key.

India Vincent: I advise clients that the best way to limit the risk of an attack is to make your business a less desirable target. And the more data you maintain, the more desirable you are as a target. If you don't need it, don't keep it. A lot of businesses have a mindset of retaining data indefinitely because data is valuable for a variety of reasons. Understanding what data is necessary for the operation of your business, and limiting the data you collect and store to the data necessary for the business, can make you less likely to suffer an attack.

Mike Roman: Simply elevate employee awareness of the exposure that's out there. The scams and the phishing attempts that are happening, so much of it nowadays involves the human element and the susceptibility of employees to click on a link that's fraudulent. So take some action to just start employees thinking about being more careful.

Jordon Cochran: The first step is to fully understand your company's exposure to attack. What does your cyber infrastructure or terrain entail, specifically the boundary – the part that's internally exposed versus externally exposed to attack – and what is the cyber security posture of that infrastructure? Does this electronic company boundary include in-depth defense mechanisms, such as firewalls, intrusion protection systems and intrusion detection systems? Finally, who do you have ensuring these critical assets are continuously monitored, updated and defended? Are key access points such as locked closets and rooms properly secured physically, with restricted access on a need-to-access-only basis?

Conrad Bell: One of the most important and effective things that can be done to reduce risk is to establish a comprehensive security awareness program. Even with the best technical protections in place, there are no guarantees that you will not become a victim of ransomware attack, data breach or other cyber threats. Unfortunately, users are the weakest link in cybersecurity. Therefore, it is important to address the user impact on cybersecurity by automating security practices whenever possible, but even more importantly, creating a security awareness culture. This entails educating users on how to identify threats and react to them. Furthermore, every company should identify specific threats to its current security posture, and adjust security priorities based on risk.

Q: How serious is the threat of a cyber-attack on my company, and what are the potential consequences?

Vincent: It's a serious threat for all businesses. I read an article last fall that said your chances of having a data breach involving more than 10,000 records is greater than your chances of getting the flu. Anything that is occurring with that frequency is a serious threat to any business. For larger businesses and those with large data sets, you hear the consequences in the news on a regular basis. For smaller businesses with more limited data, a data breach has significant consequences due to the cost associated with containing the incident, remediating the systems, and complying with any notification requirements – as well as the impact on the company's reputation. If lawsuits emerge because you handled the breach improperly or were negligent in protecting the data in the first place, the consequences can be much worse.

Roman: One of the statistics I saw recently is that half of all U.S. businesses have had some type of event or breach or hack over the last three years. So at some point, it's very likely that you're going to experience a breach. There are two major ramifications. One is that it's going to cost a significant amount of money and time and resources. But

the other part is reputation. If you have a breach, what's that going to do to your reputation and brand, and your revenue going forward for the next several years?

Cochran: Cyber-attacks are extremely serious, and the costs at which it takes to pull off a compromise are negligible compared to traditional theft, warfare or physical attacks. Oftentimes, companies won't know they have been compromised until it's too late. Attacks today are very sophisticated, well-coordinated and well-funded globally. Malicious actors are continuously scanning for open vulnerabilities to gain a foothold wherever they can to wreak havoc. A recent trend has been cyber hostage or ransomware where a company's intellectual property or critical data is held hostage for money. Also, a compromise can raise serious doubts about the company's ability to protect its customers' information, which can impact market confidence in the company. The time it takes for malicious cyber actors to weaponize publicly known vulnerabilities is measured in days.

Bell: Cyber threats should be taken very seriously. At C Spire, we encourage that cybersecurity is integrated with every line of business, and in how services are delivered. From a security standpoint, it is vital that companies take a deliberate approach of protecting sensitive data by using risk-based analysis to identify gaps between people, processes, and technology. One of the potential consequences of an attack reputational damage. Loss of customer trust can be the most harmful impact of a cyber-attack, especially if there was associated unauthorized access to customers' data. This will likely translate into a loss of current business, as well as future prospects. In addition, depending of the scope and type of the cyber-attack, heavy monetary penalties may be levied if you fail to comply with data protection regulations such as HIPAA, PCI or state/federal guidance. And there is the economic costs of incident response and recovery. The impact of operational disruption is often underestimated. Budgets for resilience and continuity strategies may not account for all contingencies. Certain situations my hinder the ability to maintain revenue, and insurance premiums will most likely increase.

Perry: A fundamental tenant of cyber security is that a breach is going to happen, and no matter what you do to try to prevent it, you're never going to be 100 percent protected. That goes for all businesses. The amount of data that you have indicates how likely you are to be attacked. But it's not just the data you have, it's also the people you have. Some reports from the FBI say that some of the cyber events from other countries are not on our data so much as on the people, and trying to get the people to turn and send information. It's still a breach of information, but they're going after people and not the actual data within the organization. They get the data through the people. That's where employee education comes in.

Q: What are some of the key components of a plan to reduce my chances of being hit by a cyber-attack?

Roman: The biggest thing is to take some action. So many companies out there are doing nothing. Take some steps, even if it's baby steps. But do something. Form a committee to talk about where your data is and how you transmit it. Start training your employees to recognize and think about those scams that are out there, and to be more careful at work. Beyond that, there are a lot of resources on the Internet, as well as third-party providers that can help you with structuring the IT side: the hardware, software, protocol and procedures.

Cochran: A business continuity plan, data backup, a restoral plan and implementation, and a continuity of operation plan, or COOP.

Bell: An effective cyber security plan should begin with getting basic security in order. This includes access management, creating a vulnerability management program for patching and remediation, and cyber security awareness training. Next, internal stakeholders should collaborate to select and work within a security framework that best supports future security and business objectives. The security professionals in your organization should be aware of the latest threat intelligence and have an understanding of regulatory factors and general liability that effect security controls. Also, a thorough risk assessment should be conducted to ensure security gaps are identified. Finally, companies should implement an incident response plan.

Perry: The key components are those security measures and general controls that you can implement in your organization from an IT perspective to try and protect your business. But it's not a one-and-done. You have to continue it. You have to do something different every day to add to it. But like Mike said, it's baby steps. Outside of large organizations, nobody has the capital to do everything at once. So prioritize, and after five years you have a nice, robust IT environment. It may take a while to implement, but at least you're taking the right steps. It's some of the policies and procedures and security measures that are either in your insurance policy or in some of the data-breach notification acts that are out there.

"It is money well spent to have a third party who specializes in cyber-security vulnerability assessments or penetration testing to perform an outside-in red team attack on your company."

- Jordon Cochran

Vincent: Do something. Prioritize your efforts to implement controls, and make sure you have a plan. It doesn't have to be a fail-safe, fully robust plan on day one – or ever – but it needs to indicate that you have given the issue some thought and you know what to do when an event occurs. From a legal perspective, I usually prioritize based on what others in the industry are doing, unless there are regulations in place. Because if it becomes apparent that you were not taking even the most basic actions that the rest of an industry has already adopted, not only do you have the breach consequences to deal with, but you may also be considered negligent in your efforts to protect the data that you store. In most industries, some of those basic measures you should consider are two-factor authentication, employee training, firewalls and retaining system logs to see when and how data was transferred. Once you have those basics in place, you want to always continue improving on that plan.

Q: What types of service providers or partners can help my company assess our threats and develop a proactive plan?

Cochran: Your internet service provider can help you shield your company from many of these types of attacks. Also, it is money well spent to have a third party who specializes in cyber-security vulnerability assessments or penetration testing to perform an outside-in red team attack on your company. In addition, an insider attack scenario should be completed, where your company allows an approved red team to start on the inside of your network to look for internal areas that need to be more secure. If an insider wants to be nefarious, is the company adequately postured for this scenario? Is information available to a user who shouldn't have access to it?

Bell: There are many service providers that offer audit services and can assist in creating a protective plan. C Spire Business offers many IT security solutions, including security audits, security consulting and

managed security. When selecting a security provider, I encourage business owners and leaders to research any company they are considering for security services. Providers should have a proven track record and should have qualified and certified security professionals who can create custom plans based on your needs.

Perry: You need lawyers, insurance agents and outsourced IT assistance. You need somebody to do a risk assessment. Where are my risks? What are the issues? All those third parties look at it in a different manner. If you can have some assistance in all that, you're going to be well protected. The risk assessment will help you identify where your gaps are, your attorney will know what your plan is when a breach happens, and your insurance provider will know if and how you're protected. If you're small enough, an outsourced IT company is your backbone, and you have to know that they have the right resources in place to protect you.

Vincent: Having an IT consultant doesn't mean you don't need an insurance agent or a lawyer. All these professionals have different viewpoints, and you will need a pre-existing and working relationship with all of them in the event of a breach. When the breach occurs, you will be in a much better position if you have already worked with all these professionals and they know your business and your response plan, so you don't lose those first critical hours sorting out what everyone is going to do and how they are going to work together. When you do have to activate that plan, call your lawyer first because the lawyer will help you maintain the attorney-client privilege for as many of the conversations as possible.

Roman: If you're a small company, you might not have a dedicated attorney on staff or on retainer. But if you're a little bit larger, you're going to have an attorney and accounting and insurance brokers and an IT company that are all sitting there, and they know a lot of stuff. They've seen a lot of the claims. So take some action. If you simply had a dinner or a lunch where you got all the groups together and talked to them and took some notes, that would be a huge step towards doing the right thing.

Q: What types of questions should I ask when assessing my cyber risk or choosing a third-party partner to help improve my cyber security?

Bell: What are the critical systems and data? How is Data stored and accessed? What is the impact to business if corporate or consumer data is destroyed or exposed? What are the industry best practices? What cyber security framework is being used that is reflective to the current business operations?

Perry: It's all about vendor management. You cannot outsource responsibility. I can get somebody else to hold my data, run my payroll and do the processing. But it is still my responsibility to make sure they have good controls in place. So you need to be asking, "What controls do you have in place to protect our information?" In regard to the third-parties, get someone who has done this before. Your general counsel is not going to be the person you're going to call when you have a breach. You need somebody who is an expert and has seen this and understands it. The biggest questions that need to be asked are, "Have you done this? What is your expertise and experience in this?" And that's really just your own vendor management.

"It is amazing how much you can do in-house just by Googling and spending an hour or two with your leadership team."

- Mike Roman

Vincent: When you evaluate partners in the cybersecurity space, the questions are similar to those you would ask in other fields. In practice, there are some cybersecurity questions you should be asking most vendors, even those not specifically providing IT services. Some of those key questions are: "How much experience do you have providing this service? Do your people have the right certifications and experience? Who will be personally handling this for my business? What type of track record do you have?" You also want to know if your vendors have their own insurance, both to cover their mistakes and to protect you and the vendor in the event that the vendor's system is the one that is breached. To the extent that the vendor is a critical portion of your infrastructure, you also want to be sure that your agreement gives you clear insight into the vendor's operations should you need it. In the event of a breach involving the vendor's system, be sure that the vendor will provide you with copies of all necessary logs and other system information you may need to fully diagnose the scope and impact of the incident.

Roman: A lot of our companies – being a little bit smaller in the mid-market space – outsource their platform, their software as a service, or their websites. So what happens is they probably have a contract with the third-party vendor, but if there's a breach that the vendor caused, by most laws it's the responsibility of the company to notify those potentially affected individuals. It's their breach. Even though the third-party vendor may have let it happen, that doesn't matter. It's the company's responsibility. Even if you have a contract and they have insurance, if it's a really bad claim, how quickly do you think that insurance from them is going to start paying? It's going to take a while. So we tell our clients to buy insurance for themselves. That way you'll get your reimbursements right away, then you can let the insurance companies work it out. But meanwhile, you're back in business and trucking along.

Cochran: A key to this red team concept I mentioned earlier is to have trusted agents who know the entirety of the operation. That way, they know when the red team is acting maliciously, and can observe the company's cyber-security defense procedures to discern capacity and capability to defend the company's assets by the personnel on hand assigned to perform these duties.

Q: What are some of the legal ramifications my company faces when it comes to protecting my customers' secure information against cyber threats?

Roman: Probably the top one is notification requirements. All 50 states have state notification laws, and they all differ. If you have individuals in 35 or 40 states who have been affected by your breach, it's going to take a lot of legal forensics to wade through the law in each state and figure out what you have to do to comply. Added on to that, if you have protected health information, the federal government through HIPAA and the Office for Civil Rights is going to come in and say that by law you must notify all these people. Beyond that, if it's a bad breach and you face a class-action type of lawsuit, or if you were negligent and didn't put in reasonable controls, you can potentially face some backlash. Although historically what I've seen is that until those individuals suffer damage, the claims against the organizations for letting the information get out there haven't really gone very far.

Cochran: Many types of data require certain types of protections, including financial records, personally identifiable information, and personal health information. These protections include actions when the data is in-transit, or at-rest in a data warehouse. Also, there are state and federal reporting requirements if a cyber breach is experienced if certain types of information are involved, such as personally identifiable information.

Perry: The legal ramifications of a cyber event versus a breach are different. That becomes a definition perspective from the organization.

Because you can have an event that is not a breach, and that has a different track to it. Most people go straight to the worse thing, the breach. But once you start pulling back the layers you may realize that it really wasn't a breach, and in that case you don't have to notify anyone. So the legal ramifications really depend on what type of event it is and the magnitude of that event. You have to stay on top of that, and you need to have somebody who understands just that piece. Your general counsel is not the person to call if you have an issue. Instead, get a cyber-experienced attorney to assist in this area.

Vincent: That difference between an incident or event and a breach is very important. If you decide that your business had an incident, then you need to carefully document why you decided it was an incident and not a breach. That analysis needs to be retained so it is available years later if someone asserts a claim that you failed to notify according to the legal standards. In terms of claims, once you have worked with law enforcement if necessary, remediated your systems, handled any notification requirements, and begun working to repair any reputation damage, the largest remaining legal consequence is any litigation that might arise. Mike is correct that individual claims are not gaining much traction these days unless the individual has actually been damaged, but changing legal standards mean this could always change. At the same time, litigation with service providers and customers, as well as banks and credit card providers, is more likely to result in significant damages.

Roman: It's important to note that individuals can still file those lawsuits, and it's going to cost you to defend it, even though you may prevail.

Vincent: There is also the possibility of hope on the horizon when it comes to navigating regulations from all 50 states. There is currently a lot of discussion and negotiation related to development of a single federal regulation for data privacy. It would be nice if the outcome of those efforts is a single regulation that applies across the board and eliminates different requirements from each of the states.

Bell: Government fines, penalties and even jail time in extreme circumstances are some of the consequences of not protecting personally identifiable information adequately. There is also the cost of litigation associated with mishandling of personal data. Governmental notifications and penalties may also apply and may differ within state, federal or international jurisdictions.

"You cannot overeducate when it comes to cyber security."

- Paul Perry

Q: How can my company be proactive when it comes to educating employees and helping them reduce the risk of a cyber breach at my business?

Perry: I'm going to steal a tagline from real estate and retail: education, education, education. And when we're done with that, you add in education, education, education. Most people don't listen to the education until it actually involves them. You have to hear it again and again, and then one more time for good measure, because that's the biggest piece. It doesn't matter how you educate: annual meetings, company intranet posts, mandatory video education with online testing, etc. It doesn't matter if it's monthly or quarterly, or if it's printing out a phishing email and everybody discusses it. You cannot overeducate when it comes to cyber security.

Vincent: I agree that the employee training is absolutely critical, but I will take it a step further and say those who have the resources to do so should evaluate the extent to which the employees and contractors understood and processed the training. Particularly if you're not doing the training in a live setting – if you're letting them do it online at their desk – most people are easily distracted during training unless they know they are responsible for learning the material. Doing some sort of evaluation to see if the key points are starting to stick in each person's mind, and having follow-up options if a particular concept is not understood, can greatly increase the value of your training. Evaluations can take a variety of forms, including questions immediately following the session, fake phishing emails after the fact, or other simulated incidents to see how employees will react. Whatever you choose, the more exposure employees have to the issues, the better the chance they will be an asset in stopping or limiting the scope of an attack.

Roman: The education and training are absolutely number one. If you can afford it, there are companies out there that will help you with some training, putting out fake emails to your company to see who falls for the deception and clicks through. There's a company here in Birmingham called ThreatAdvice that does exactly that. They will send some emails out, and you will find out exactly who's falling

for those attempts. Then you can zero in and laser your training for that particular group of employees. It is amazing how much you can do in-house just by Googling and spending an hour or two with your leadership team. It's eye-opening. That alone will probably ward off an event or two. But if you have the financial resources to hire an outside firm, that's really helpful.

Bell: Cyber security awareness training should be relevant to staff and their particular job role. Regular mandated sessions with employees should explore different types of social engineering and cyber-attack exploit scenarios to help them better understand and recognize any potential attacks. It should also be emphasized that cyber security is also relevant outside of the workplace at home and on mobile devices. C Spire business is conducting a free Cybersecurity Awareness Training via webinar on Feb. 26th. Visit cspire.com/business for more information or to register.

Cochran: This concept must start with company leadership and management and be top-down. Recurring information sharing or training should be required for employee awareness, and the company should have an acceptable-use policy for company computer and information resources. Also, it's important to share information and best practices and training for employees and their home use, as they may work remotely or transfer files from home to work. If employees at home have a much less secure configuration and a higher level of risk, then that can translate directly into risk to the company.

Perry: I agree that it starts with management and the owners and leadership. They have to buy into it. If we're having education training and the CEO and CFO aren't sitting in the front row, then most people won't understand the importance of the training and could dismiss it. They need to see that the leadership cares and it's the culture you've created. So it's definitely important to have leadership involved. Then thinking beyond just online breaches, I have a client who will come in and see how far into the organization they can get by using fake badges or carrying boxes and seeing what door they can get into. It's more social engineering from that perspective. Then you can come back and show people where security measures failed.

Q: What are some best practices to help monitor for and identify breaches? What are the key components to be included in a breach/incident response plan?

Vincent: For monitoring practices, any type of monitoring that will help you look for anything unusual in your system. Depending on your business, you expect different behaviors in your system. Checking logs, firewalls, system activity, volume of uploading or downloading, or other metrics for anything outside of the baseline can help you identify a breach. If it's not normal for a particular employee to download 200 documents in one day or to upload any information to the system, and he or she does, then you may want to look into that. Just make sure you have the ability to monitor any tracking systems you put in place, because sometimes businesses don't have the resources to track every different way an attack could happen. Key components of a response plan start with identifying who your response team will be. Once you have the team identified, determining who has which responsibilities and who has what authority is key. You don't want to spend time in the middle of a breach figuring out who has the authority to make a decision. Both the team and the company management need to be aware of this team and the assigned responsibilities. Defining those individuals and their responsibilities will naturally flesh out a good part of your response plan. Make sure that any tools needed to implement your plan – such as incident investigation checklists, contact lists, and documentation guidelines – are easily accessible somewhere other than on the computer system.

"In order to properly handle a situation related to a current employee, there must be significant guidance from and involvement with human resources and legal counsel, beyond just addressing the technical concern."

- India Vincent

Roman: The minimum thing you need to do is sit down and talk about it and formalize some type of plan for monitoring and identifying breaches, and then the following response. Just sit down and have a 30-minute conversation about – if you do have an event – who's going to do what, who gets notified, and who has the authority to do X, Y and Z? I'm such an advocate for having a cyber insurance policy in place, because most companies don't have the resources either financially or internally to have a response team. With a cyber insurance policy, the cyber-breach coach already has the forensics, legal and other vendors for identity-theft monitoring, credit monitoring and notification services. They already have all this organized. So when you're panicking as a company because you just had an event, it's no problem. Just pick up the phone and you'll be connected with the breach coach. They've been through a thousand claims. They know what you're going through, and they'll be able to help. Even beyond the money aspect of an insurance policy, having an organized breach coach is the best thing that will come out of it.

Cochran: A key for this is to know what a baseline of network activity looks like. It's important to invest adequately in the tools that can protect a company's information. Another key partnership is to subscribe to the Department of Homeland Security's Cyber Information Sharing and Collaboration Program. Finally, it's helpful to have tools that can correlate behavioral aspects of the acceptable-use policy – such as typical work hours and work actions – and alert requisite management when abuses are flagged. This includes employees working odd hours, excessively sharing drive access, printing excessively, etc.

Bell: Best practices including educating and training employees to be able to identify indications of a possible breach; deploying a data loss prevention system security professionals to establish rules for accessing sensitive information, keeping unauthorized users from sharing data maliciously; identifying a network traffic baseline to be able to identify what is not normal; monitoring for the presence of unknown or unauthorized IP addresses on wireless networks; and monitoring for multiple failed login attempts for system authentication, especially after-hours. The key components in a breach/incident response plan should include a chain of command for the incident response team to ensure minimum confusion, a clear communication plan, and a clear definition of what defines a breach/incident. This plan should be tested regularly.

Perry: Know your business. You can get a bunch of reports out of a protection system or a monitoring system. You should read those right away. Because if something seems unusual it probably is, and you need to investigate it. A lot of organizations that have breaches, they had kind of a head-in-the-sand mentality. They said, "Oh, I have all this stuff in place. I don't have to monitor it." That's when you lose sight of truly noticing when a breach has occurred.

Vincent: While the numbers vary a little depending on the source, statistics right now indicate that it takes an average of around 200 days to identify a breach. That makes the ability to review reports from your monitoring system in real time vital to identifying and containing a breach.

Perry: That statistic is why it's important to change your password every 90 days.

Q: What are some often overlooked areas of potential cyber risk that my business should consider?

Cochran: It is important to fully exercise the company's Business Continuity Plan, not just table-top exercise it. This includes the continuity of operation plan, where applicable. It is also beneficial to subsidize a commercially available anti-virus software for employee home use.

Bell: Mobilization of data to smart phone personal cloud accounts is one of the most overlooked and growing risks. There is a lot of configuration management that must be put into place to ensure data is being stored in the appropriate place. Also, with the increasing need to ensure confidentiality of data, more emphasis should be placed on encryption key management. Sloppy protection, storage, back up and organization of encryption keys increases cyber risk.

Roman: Cyber insurance, unfortunately, is often overlooked and not purchased. Many businesses think they won't experience an event because they have a firewall and antivirus software; or that they don't have an exposure because they don't have personal information on others. The reality is that if you have even one employee, you have an exposure. Most businesses are more likely to have a cyber event than have their building burn down, yet they buy fire insurance and don't buy cyber coverage. This is important insurance, and it's really good these days. The policies are very broad and they're getting less expensive. I still see companies that are not buying a cyber policy, and it baffles me.

Perry: As we do IT control reviews and audits, we see a lot of common deficiencies amongst all companies, and lack of education is at the top of the list. The other biggest deficiency we see is where terminated employees still have access to the system. It only takes one, and there is nobody more disgruntled that a terminated employee who knows they still have access to the system and can wreak havoc amongst your business and really kind of take you down. Little things like that are often overlooked. If I have a checklist for terminating an employee, make sure that removing his or her access to the system and bank accounts is on that checklist. Other common deficiencies we see are weak passwords and passwords that never change.

Vincent: I agree that access for a recently terminated employee is often overlooked. Beyond that, companies are often completely unaware of the risk posed by an unhappy, still-

employed individual. Response plans do not usually cover this issue. In order to properly handle a situation related to a current employee, there must be significant guidance from and involvement with human resources and legal counsel, beyond just addressing the technical concern. Because of the additional complexities involved in these situations, the scenario is often left out of response plans or only briefly touched on. Limited treatment of the issue in a response plan may be appropriate, but the human, technical and legal resources that will be called upon in that situation should be aware of their roles and have a common understanding of the considerations involved to protect the business and preserve the individual rights of the employee.

Q: What is the outlook like for cybersecurity moving forward? Are threats to my business only going to increase?

Bell: Cyber security demand will only increase because the cyber landscape is rapidly changing. Enormous data collection, 5G networks, cloud computing and the Internet of Things are all changing the scope and increasing the number of threats to consider.

Perry: By next year there's expected to be $3 trillion in losses for organizations, and that's grown substantially over the last two years. The outlook is that we can never go on the offensive, we always have to be on the defensive. And, as the cyber criminals get better, we have to keep up with them. It's probably going to take a "death by a cyber-attack" to really open people's eyes and make this a focus by the federal government. That's a scary thought, and I don't mean to be doom-and-gloom. As the world becomes smaller as we're connecting through technology, it just opens us up more for that type of outlook. We just have to keep doing something proactive every single day, keep educating the masses on the right things and wrong things to do, and be diligent with what we have.

"Cyber security demand will only increase because the cyber landscape is rapidly changing."

- Conrad Bell

Vincent: It's true that businesses and individuals will always be on the defensive in this field. The attackers only have to be successful once to damage a company's finances and reputation, but the business has to be successful in identification and containment each time an attack occurs. With the Internet of Things continuing to grow and the number of connected devices exploding, threats can materialize in even more directions. Every time you get a new thermostat control for the office or a new conference-room scheduler, or your employees begin reviewing their email on their smart watches or through voice-to-text options on their smart devices, you introduce new access points for an attack on your system. Keeping up with all the new office conveniences is often in conflict with maintaining the security of the company's computer systems, and security professionals must work with management to find a balance with an acceptable level of risk.

Roman: The reality is the outlook is bleak. It's certainly going to get worse and more prevalent, and have more of an impact on all of us in the country. I am particularly concerned about the Internet of Things. If my firm gets shut down for several days, it's going to be painful and we're going to have to spend some money and do some things to clean it up. But if a dialysis machine in a hospital gets quarantined by a hacker who says they're not going to let it run until you pay them, and that patient dies, now you're talking about a whole new level. So the Internet of Things is daunting and scary from that perspective.

Perry: You cannot have both convenience and privacy. Unfortunately, you have to pick one. As the Internet gets bigger and the Internet of Things becomes more mainstream, those create convenience and it gets away from privacy. And we have to choose. Are we okay with giving up privacy for convenience? It wouldn't surprise me to see us go backwards in the next 10 years and say we'd much rather have privacy.

Roman: And we shouldn't ignore the exposure on a personal front. What if the CEO of your company gets hit massively by some type of personal hacking incident? You know how busy he or she is going to be over the next six months repairing their credit and bank accounts? Are they going to be helpful to the company during that time?

Cochran: The bottom line is that cyber-attacks will continue to increase in sophistication and volume, especially with the cost of entry to perform these attacks being very minimal compared to the significant reward or return being so high. As a result, companies must invest appropriately in the security of their corporate information and resources.