BIRMINGHAM BUSINESS JOURNAL

TABLE of EXPERTS Series

Insights into CYBER SECURITY

The Experts

Jason Asbury

Warren Averett Technology Group

Jason Asbury is a Member of the Firm and serves as President of Warren Averett Technology Group. He has more than 15 years of experience working in the IT industry. Jason has worked in an advanced technical capacity as a systems engineer, and has had a primary focus in IT consulting. He has been heavily involved in implementations and management of multiple patient care systems and associated medical management applications including EMR, Practice Management, PACS, Lab Information Systems, IMH, Telemetry, Clearing Houses and Oncology Radiation Systems. He maintains a unique skillset including experience providing consulting services and managing projects for clients in the fields of banking, insurance, education and law. Jason worked in an advanced technical capacity as a systems engineer for Science Applications International Corporation and served as an operations executive in the managed services and project implementations consulting arena for six years. As President of Warren Averett Technology Group he is responsible for the day-to-day management of the company and its overall direction with regard to strategic growth and planning.

Brian Jackson

Abacus IT Solutions

Brian serves as the President and Chief Operating Office of Abacus IT Solutions. In this role he oversees all executive decisions and operations of the company along with providing client solutions and client development.

With over 15 years of experience, Brian has been able to use his knowledge of Accounting and Technology to provide client technical solutions across various organizations and industries.

He began his career in technology by implementing accounting systems, business intelligence Solutions, and developing system integrations. Brian now works with clients to implement and support business applications, as well as the computer hardware, network infrastructure, cloud solutions and cybersecurity.

Andy Obuchowski, Jr.

RSM McGladrey

Andrew Obuchowski is the national leader and supports global operations for cybercrime and data breach investigations, digital forensics and incident response services within the security and privacy consulting group. Andrew possesses more than 20 years of experience, including 12 years of law enforcement investigations, instruction at numerous police academies, and long-time memberships in several computer and financial crime task forces. He is also currently an adjunct professor of criminal justice at Anna Maria College in Massachusetts, where he developed and teaches graduate and undergraduate programs in information security, digital forensics and cybercrime investigations.

As an industry leader and expert in his field, his team provides services and solutions for clients in preparation of and in response to matters involving a wide range of information security and privacy assessments and investigations.

David Powell

TekLinks

David Powell is a 17 year veteran of the IT industry, the last 12 spent exclusively in Managed and Cloud Services. Named one of the Top 250 People in Managed Services by MSPMentor for four consecutive years, David has worked for 3 of the top 100 Managed Services Providers. Since coming to TekLinks, he has helped transition TekLinks from a traditional VAR to a company with a nationally recognized Managed and Cloud Services practice. TekLinks received the Top MSP award from CRN at the VAR500 awards in both 2010 and 2012. David is a frequent speaker on technology and managed/cloud services. Additionally, he has a "Tech Tuesday" segment that airs each week on the local CBS affiliate in Birmingham.   He was recognized in 2011 by the Birmingham Business Journal as one of the Top 40 under 40. In 2013, he was recognized by the Birmingham Business Journal in their first ever ranking of the #40toFollow in Birmingham, recognizing David as one of the top 40 people in Birmingham to follow on Twitter.

Ken Sawyer

Sawyer Solutions

Ken Sawyer is a native of Mobile, AL and holds a Master of Engineering from the University of Alabama at Birmingham.

With over thirty years of experience, Ken has served in many capacities in the Information Technology industry. He has worked for multi-national corporations and been a part of numerous technology startups. He is currently a Certified Information Systems Security Professional (CISSP), a Project Management Professional (PMP), a Microsoft Certified Solutions Developer (MCSD), and a Certified ScrumMaster (CSM).

Ken is the CEO of Sawyer Solutions which provides managed security and IT services, software development and consulting. He is also a proud member of InfraGard and the Information Systems Security Association (ISSA).

India E. Vincent

Burr & Forman

India Vincent is a Partner at Burr & Forman focusing on intellectual property, cybersecurity and technology, business planning, and corporate transactions. India assists clients in all industries with developing security and data protection policies and breach response plans.

In addition to cybersecurity and data protection, she assists clients in developing, managing and selling their businesses with a specific focus on maximizing the value of intellectual property assets. India works with clients to determine appropriate strategies for protecting, licensing and enforcing their intellectual property, including trademarks, service marks, patents, trade secrets, and copyrights, and advises clients regarding contractual relationships with customers and vendors. She is also admitted to the U.S. Trademark and Patent Office.

The Discussion

Q: A number of large retailers have been impacted by data breaches in recent years. How serious is the risk for small businesses?

Brian Jackson: Small businesses are probably more at risk than most enterprise businesses. I saw one statistic that 71 percent of cyber-attacks occur in businesses with fewer than 100 employees. So the risk for them is really great, and a lot of times they don't know that it is. It's not just the risk that is important to them, it's also the impact. Larger companies have cyber-attacks, and they take a hit on their stock price and get some bad press. But for small businesses, the impact can be devastating. I saw another statistic that said about half the people who see a cyber-attack occur on a business they interact with will quit doing business with them. So the risk is greater that it will happen to small businesses, and the impact is more severe.

David Powell: The risk is absolutely serious for small businesses. It's not a matter of if something will happen to your business but a matter of when. The threat profile of the large businesses makes them a more likely targets because there's more value embedded in that organization, so the risk profile for them is higher. But their resources to address their problems are also higher. A smaller business has a smaller risk profile, but they have a fraction of the resources to do something about it. So they need to begin to think across the entire threat profile and how to mitigate individual risk points, whether it's a disgruntled employee or an outside influence or whatever it may be. The small business really needs to apply time and energy around thinking about those things, and then address those risks that they identify.

Ken Sawyer: If small businesses don't have the resources to deal with data security, then they may not even be aware that the threats exist. And their ability to bounce back after any attack is severely limited. Another thing we've seen is small businesses can be attacked and become a venue into larger organizations, because the defenses just aren't there. The Target breach in 2013 started with an HVAC contractor.

Andy Obuchowski, Jr.: When it comes to small businesses, the resources and budgets are not available to have all the latest and greatest technology. So they become more like low-hanging fruit when it comes to attacks.

Jason Asbury: The risk for small businesses is just as great as it is for large organizations, and the consequences are more severe. Smaller organizations are less equipped to manage an incident from a dollars-and-cents point of view. I'm dealing with a client – a small mom-and-pop organization – that has experienced a breach relative to credit cards. They're looking at an expense in excess of $50,000 to remediate, which is multiplied by each location, and they have 11 locations. So in terms of consequence, it's even more impactful for them.

India E. Vincent: Data breaches are a serious risk for all sizes of businesses because any business can have data that a hacker will find valuable. Small businesses can be more attractive targets for a hacker because they have less security, even though they may not have as much data. If the data they do have has value to the hacker, they are a target. Research shows that a high percentage of small to medium size businesses have suffered cyber-intrusions, but they either went undetected or unreported.

Q: What can my business do to reduce the likelihood of a cyber-attack?

Powell: Ultimately the answer is to do something. The largest threat to a small business is inaction. The problem to some degree is that in the technology space, we've come in and done assessments and told the customers how badly they're handling this. And what that sometimes does is create inaction. It's like why some people are reluctant to go see a financial advisor, because the advisor tells you that you're not saving enough, you shouldn't have bought that car, your kids are not going to be able to go to college. And you're like, "Well forget it. I can't do any of that. So I'm going to buy a big-screen TV on my way home so I'll feel better." A lot of times the small business gets overwhelmed by the security profile, and that creates inaction because they think they can never address all that. The message to the small business needs to be, “Here are gradual steps you can take to increasingly become more secure.” You are never going to go from being not secure to being totally secure. It’s not a binary thing. It’s like being healthy. You take steps to increasingly become healthier. You take steps to increasingly become more financially secure. So the way we want to have this conversation with customers is for them to do something. Begin to look at what the overall threat profile looks like, and then take reasonable steps to increasingly become more secure. Get on the journey and start moving towards a more secure environment.

Sawyer: There’s really nothing they can do to reduce the likelihood of an attack. They’re under attack all the time, every day. The idea is to prevent the attacks from being successful. We’re all deluged with malware in terms of email and bad websites. They’re all over the place. So you need to take the basic steps. The studies continuously show that investing in the very basics has the greatest return. Do the low-hanging fruit first, the simple things. Put anti-virus on all the computers, add patch management, a little bit of access control. Some of the really basic things can be that first step. But do something. Develop a path. Many of the basic things are very inexpensive. We’re not talking about a huge amount of money, maybe $10 to $15 per computer for a good start.

Obuchowski: There are five things that organizations can do. One is understanding your network and the risk that you have, so we’re talking about a risk assessment. Second, know the information that you are storing and receiving, and make sure that information is protected. Another option is to do network-vulnerability testing. I like to use the term, “Trust, but verify.” There are network testing tools out there to identify vulnerabilities and make sure that the open doors and windows to your organization are closed. Vendor management is also very key when it comes to smaller businesses, because everything tends to be outsourced, everything is moved to the cloud. When you’re involving everybody else in order to help protect your organization, vendor management comes into play. So make sure the vendors you’re working with also assume the best practices that you’re implementing. Lastly, you can spend hundreds of thousands of dollars on cyber-security products, but all it takes is one employee to be sitting in a cubicle somewhere in the office to basically bring down your entire network. So security-awareness training is also important, or as we like to call it, securing the human. Forget about the network; secure the person. Then take into consideration that when you do have an incident, how are you going to react? Make sure you have an incident response plan.

Asbury: First and foremost, in order to manage risk, key stakeholders have to recognize and acknowledge that risk does exist for their organization. If that requirement is not met and leadership doesn’t really acknowledge that there needs to be a proactive approach to security, then most organizations are going to have a hard time successfully securing and preventing a breach. The general concept and approach should be proactive, to ensure that an organization is doing as much as possible to eliminate the need to be reactive. That includes regular vulnerability scanning at least on a quarterly basis and annual penetration testing. Additionally, a clear security plan that addresses endpoint management, user access, system administration and incident response is a foundational necessity for reducing exposure and preventing a breach.

“First of all, the business can’t be ignorant about being attacked. They’re going to be a target. They can’t assume that they’re too small or insignificant to be a target.”

- Brian Jackson

Vincent: Given the current cyber landscape, it is not unreasonable to think that all companies will be victims of an attack at some point, regardless of the steps they take. The objective, then, is to take steps to minimize the impact such an attack would have on your customers and your business. At a high level, the most important thing for all businesses to do is to understand at least the general nature of the threat and to make informed judgments about what data to secure and how to secure it. It is not reasonable to expect small businesses to be able to undertake all the security measures a large, international company would. But at the same time, if the small business has particularly sensitive data, it will be expected to spend additional resources to protect that data. Understanding the type of attack most likely to be used on the business (phishing, DDOS, Advanced Persistent Threats, just as examples) can help determine the best course of action to protect the data.

Jackson: First of all, the business can’t be ignorant about being attacked. They’re going to be a target. They can’t assume that they’re too small or insignificant to be a target. It has to be an organizational effort. Everyone in the enterprise has to make a conscious effort to reduce the likelihood of an attack. That means being diligent in how they interact with any online resources that they access. We can put a lot of technical security tools in place, but all it takes is that user who wants to save 5 percent on their next Kohl’s purchase. And they click on that link or attachment, and it breaks down all that money you spent on technology to protect your network. There is no 100-percent foolproof technical solution. User education must be one of the core focuses that small businesses need to make. It’s a combined effort, and a lot of diligence needs to take place to reduce the risk of something happening.

Q: What are the key ingredients for a strong small business cyber-security plan?

Sawyer: Every business is different, so it’s something that is going to need to be developed on an individual basis for the business to determine where their greatest risks are. We know the basics always need to be covered, and some businesses aren’t doing those. So different businesses are going to have different starting points. There has to definitely be buy-in from the top of the business, but also buy-in from the bottom. There really needs to be a concept of how this is going to benefit the enterprise, and employee engagement is essential to this. If you don’t get the people in the trenches involved, then they don’t understand how this benefits them or what the risk is. If there’s a breach and it costs $50,000, how does that impact their job security? So the cyber-security plan needs to involve everyone within the business to understand the exposures. Some response plans can be very simply where you just call one person. Other plans can be very complex. But it has to be something that works for the business. A plan that gets developed and then put on the shelf is of absolutely no value. So even if it’s only one paragraph that they can actually do, that’s what needs to be concentrated on. Something that will actually work for that business.

Obuchowski: This is not an IT Department issue. It is a holistic approach from the top down across all different groups within the business. That’s the key factor here, understanding that the whole organization has to be proactive when it comes to protecting information. It’s not just an IT problem that they need to fix.

Asbury: I like to talk to my clients about safeguards, and the Department of Health and Human Services really did a good job defining those safeguards and categorizing them into three buckets. They are physical, technical and administrative. Physical safeguards deal with physically securing your data. Technical deals with using technology in an effective way to manage security. The administrative component is what most organizations overlook. It deals with the documentation of policies and procedures, and then the communication of those policies and procedures. I couldn't agree more about needing to have buy-in from the bottom as well as the top. It's important for organizations to understand that there's a need to communicate to all the users in a particular system. There's a term that's been coined by the PCI (Payment Card Industry) Security Standards Council that's called BAU: business as usual. What that means is you communicate changes in policy or a security plan as things change in an organization. So business as usual means if new users are added or new systems are introduced to an organization, those administrative components are communicated. Good ways to do that are through emails, videos and at least semi-annual training. Take advantage of company events when employees are pulled together to talk through what has changed in the organization and how to be prepared to mitigate risk.

Vincent: First, identify the data the business has that a hacker would find valuable. Is it customers' personal data, trade secrets, the company's financial information? Then retain only the data required for business purposes. If the data is not in your system, it can't be stolen during a breach. Use up-to-date operating systems and software and keep them updated and patched in a timely fashion. Use intrusion protection devices, including virus and malware protection, firewalls, and encryption if appropriate, and keep them up to date. Use complex passwords and maintain passwords in the appropriate manner. Passwords should not be on notepads under a keyboard, left with an administrative assistant or on a document on your computer. And train employees to understand and spot risks. Despite all the technological threats, a very high percentage of breaches continue to have a human act that makes them possible, such as clicking on a link in a suspicious email or downloading software from a questionable website. Even with training, employees will always be one of the biggest risks.

Jackson: We talk about it being a holistic approach and an enterprise issue. To go a step further than that, one key ingredient would be to build a culture of security in your business environment. That way everybody participates, understands and educated about the different risks that are there just for that specific business. Once everyone has that culture and it's engrained in them, they're more likely to be aware of what's going on and to avoid any type of risky behavior online or within the applications. Social engineering is a big issue with users, and that's one of the primary avenues where many businesses get attacked. So you have to build a culture of security and make people aware of what threats are out there. And you have to boil it down to what's a threat to your business. You don't want to over-emphasize certain areas and put resources in those areas that really aren't going to affect you. That's important to small businesses, because they have limited resources.

"Don't just train once and consider it done and not revisit. There has to be that continued approach of ensuring that users and employees are aware of certain protocols and procedures."

- Jason Asbury

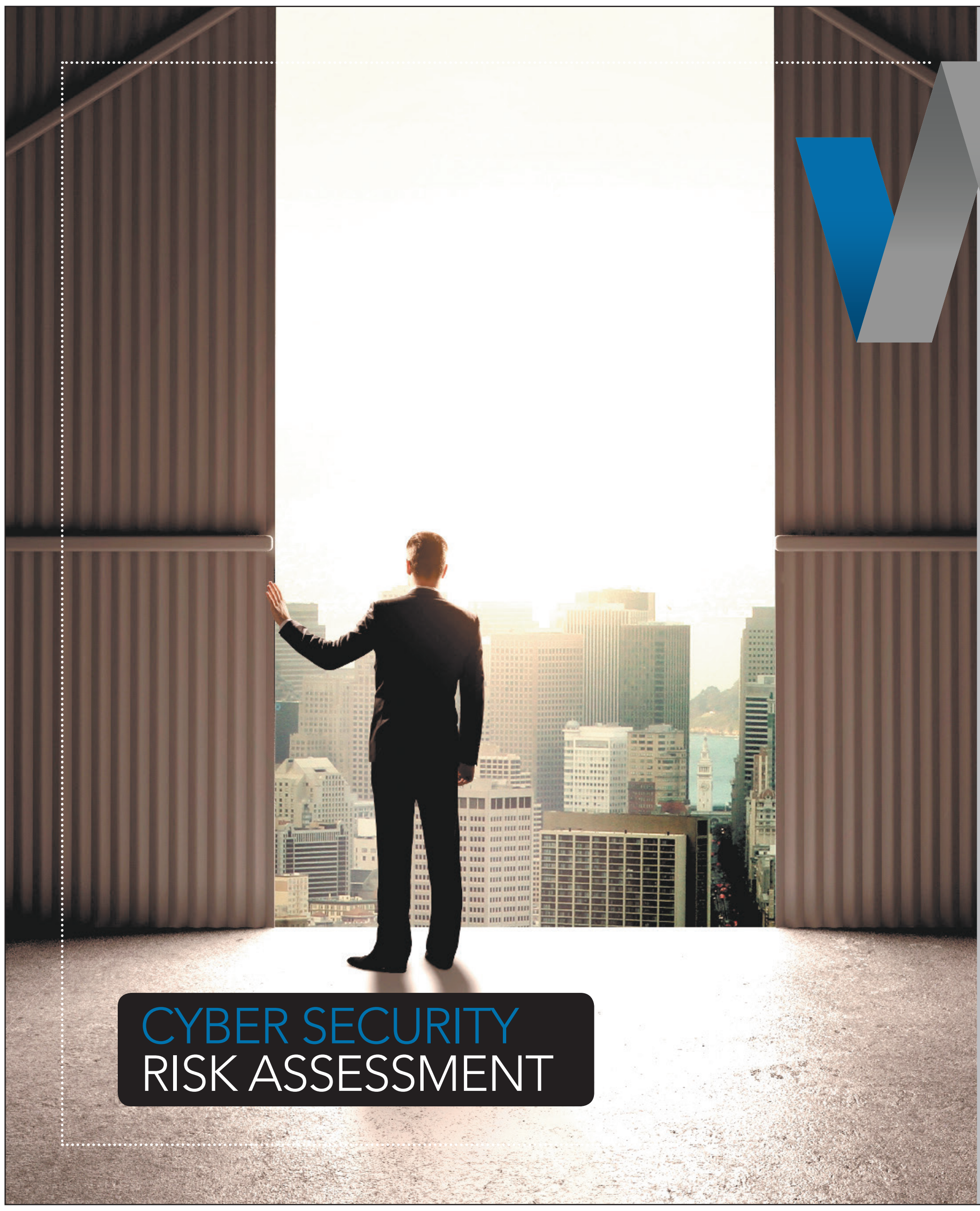
Powell: I'd like to re-emphasize that idea of a culture of security. There are some really easy things you can do to draw people into the process. A lot of times when the risk-manager meets with somebody, it feels like a forced march to this destination. As opposed to putting your arm around them and walking them toward something you want them to participate in. Just simple stuff. People hate strong passwords, but when you sit there and really explain to them the importance of the strong password and what it does for the organization, then they want to change it. As opposed to, "I have to change it because IT is overbearing." Or even simple points of education like, if you go to a trade show, you cannot accept a USB stick from someone you don't know. They could be filled with viruses. Little things where they begin to see the practical steps and make it real to the end user, and move them along that journey toward security. Culture and education and training, and engaging the entire organization. As opposed to it just being a function of the IT Department or just the boss lying awake at night worrying about it while everyone else is resting peacefully with their password set as 1234.

Q: Are there any laws or regulations I need to be aware of when it comes to protecting my customers' secure information?

Obuchowski: The big one when it comes to businesses – and it's not really so much a regulation but more related to foundation and structure – is the PCI requirement. For example, there are controls that protect credit card information. It also depends upon the type of business you're in. For example, HIPAA when it comes to health care. Also, different states will look at how you're protecting the data of residents of their state. Most businesses tend to feel that if you're doing business, for example, in the state of Alabama, then only laws within Alabama will apply to your organization. That's not exactly true. What's going to happen – especially if you're doing a type of e-commerce and you're obtaining information from residents of others states – is the attorney generals for those states are also going to have interest in your organization and how you're protecting their client information. So businesses need to keep in mind that just because you're doing business in one state, you're also going to be exposed to the laws in other states, especially post-incident. Essentially you could have 30 different attorney generals' offices all interested in your business.

Asbury: There are laws and regulatory requirements that really apply according to industry. PCI is something a lot of people are hearing about right now and it is relative to credit card transaction processing. There's compliance for the merchant, for the processor and for the large credit card organizations. In the health care realm, there's been the recent Omnibus ruling that's added additional rules and more clarity. There's information on privacy regulations, where 47 of the 50 states currently have legislation in place. Alabama is one of the three states with no information privacy legislation. However, there's definitely a requirement for Alabama-based companies to comply with the laws of other states. So if you're doing business in multiple states, you have to be concerned with those information privacy laws. In addition, for those government contractors doing federal work, there's a thing called the Federal Acquisition Regulation, or FAR. And within FAR, there are 20 critical access controls that are required to be met by government contractors. I dealt with an organization recently that received a deficiency FAR report, and what that basically meant was their network wasn't meeting minimal standards as it relates to security. So their contract was at risk of being suspended until they were able to prove they'd met those 20 critical access controls. And then there are laws relative to insurance organizations. Additionally, banking organizations have to follow strict sets of guidelines around regulatory compliance. This list goes on. I would encourage business leaders to spend time to study and discern what regulation applies to each applicable industry.

Vincent: There is no single law or regulation that governs all these issues throughout the United



States. So depending on your state, your industry and the scope of your business, you may have several different privacy and data security laws or regulations that you need to follow. Identifying these and staying up to date on their requirements is a key step in protecting your business. Your cyber counsel can help you identify these laws and regulations and conduct a risk assessment to see whether your current systems and policies are in compliance.

Jackson: The laws vary across states and across industry. So for a business that experiences a breach, it could be open season on their company. As you look across the landscape of the different states and all these agencies, they all have different types of laws of who you must notify, what types of services you must supply to people whose information has been compromised, and what you have to disclose in your filings about the breach. It's different across the board. And they may get hit with fines and penalties from organizations that they might not expect. The FCC hit AT&T with a big fine because in the FCC regulations it says they must comply with certain privacy standards. Small businesses could be hit in the same way from licensees and different regulatory organizations. So they have to be very careful and aware. They have to know who they must notify, what they must tell them and any kind of services they must provide to anybody who had their data compromised.

Powell: I think it's important if I'm a small business owner to get my lawyer and my technical team in the same room. Because the tendency sometimes for a small business owner is to play the mediator. He meets with the lawyer, and the lawyer tells him what his risk profile is. Then he talks to the techie, and they figure out what the plans needs to be. I really think you need to have both those parties in the same room. Because as a small business owner, you don't know enough of the questions that you need to ask as it relates to technology risk, and you're technical team may be able to fill that gap. It's going to cost, but that's OK. Go on and get the lawyer in with your techies and bring in some lunch and say, "What is my risk? What applies to me?" And your lawyer can tell you the changes that have come out around the various regulations, what you need to worry about and what's on the road map. And then your technical team can know what they need to be looking at. Getting those two seemingly disparate groups in the same room around a single purpose as to what applies to us, and how does that manifest itself in our technology infrastructure? I think that's a very important piece.

"My favorite three-letter organization is the FTC, the Federal Trade Commission. We recommend that everybody start there, because that pretty well catches everybody."

- Ken Sawyer

Sawyer: My favorite three-letter organization is the FTC, the Federal Trade Commission. We recommend that everybody start there, because that pretty well catches everybody. Even if you don't take credit cards or are not in health care, if anything crosses state lines, the Federal Trade Commission is going to get you. They also have some great publications and guidelines that are helpful. So we recommend that people start there and use that as a baseline. Because the things that they're requiring and recommending are really just best practices in our industry. Then beyond that you may need some other things, but find out what applies to you. Some are very simple. For instance, with the Federal Trade Commission, if you look at the penalties, a lot of things have to do with lost and stolen laptops that weren't encrypted. The fines for that are just tremendous. So you spend a little bit of time and money to encrypt your laptop, and it's a safe harbor. Really a pretty simple step to do. But you need to understand what the requirements are, and then develop a plan for reaching compliance. Some people aren't ever going to quite get there. Reaching total PCI compliance is difficult for many businesses. But there are ways to move in that direction and reduce that risk. So you need to find out what your exposure is and start on the path.

Q: What types of services are out there to help my company prevent or respond to a cyber-security threat or data breach?

Asbury: There are a number of services available to help companies manage security. Some examples include endpoint management, which is the management of all the connected devices within an organization, and mobile-device management, which basically allows organizations to secure mobile devices like phones and tablets. In addition to that, there are services available for 24-hour monitoring and logging. What that means is organizations engage outside vendors to log all traffic as it enters or leaves an organization, as well as traffic within an organization. Those logs are then stored and reviewed on a regular basis. There are also services available for regular – usually quarterly – vulnerability scanning, both internal and external. Additionally, there are services available for regular penetration testing. Basically, most of the components relative to the management of security and risk in an organization are available as a subscribed service. It really makes sense for smaller organizations with limited resources as it relates to an IT Department – or sometimes a lack thereof – to consider outsourcing the management of some of these recurring security measures.

Vincent: There are vendors for all areas of this industry. Some examples are: penetration or vulnerability testing to assess your systems; development of IT security plans and incident-response plans; employee education and training; and data storage, back-up, business continuity etc. These services allow you to outsource many of the activities that give rise to risk, making the contracts you have with these vendors very important because they will determine who is responsible in the event of an incident. Basically, you could contract out almost all the actions that need to be taken to secure your data, and some of those services make a lot of sense for any business, but particularly for small businesses. However, even if responsibility for maintaining the system and financial responsibility for a breach can be delegated through a contract, there can be brand and reputation damage to your business as the result of a breach – even if the vendor's systems were the ones breached – and sometimes it is impossible to recover from that damage.

If you contract with third parties for any of these services, you need to understand what your vendors are doing for you, what risks you are mitigating, and what risks you still bear.

Jackson: A company needs to have a risk assessment done to determine which service makes sense for them. A lot of service providers can handle the low-hanging fruit for these companies. There are local technology companies that provide these services, and there are also specialized cyber-security firms. It can be very expensive depending on the scope of service. It really boils down to the risk profile and what they can afford. This could determine what services they buy or engage in to help protect themselves.

Powell: What's fascinating to me is the amount of money that's flowing into R&D from the vendors in this space to address all these security concerns. We partner with Cisco, and one of their newest tools has kind of a DVR component where you can rewind in time to find who the person was that downloaded the thing that spread across 20 different devices. You want to find out what was that weak link, and their tool allows you to rewind back in time and find the initial point that it entered your environment. That wasn't even an option for us a couple of years ago. So these types of services continue to get better and better. In the industry you see spending by companies is double on security-related stuff than it is to everything else. So people who are buying servers, switches, storage, whatever, they're spending double that on security. And because of that, you're now seeing a lot more money flow through vendors to come up with better and more advanced services that you can subscribe to and consume as a service. As opposed to having to take all these different Legos and build your own thing. Just a couple of years ago the bad guys were way ahead of us, and they're always going to be a step ahead. But the gap is closing because of the amount of investment that's going into that.

Sawyer: It's a lot more effective for most businesses to spend the money on prevention rather than on trying to deal with it after the fact. And it's important to have an expert who understands the businesses and can work with the business to make sure the risk profile is addressed. For instance, data breaches are big in the news. There's a new one every week. Yet we find that many small businesses don't have effective backup. So while they're certainly at risk for a data breach, they're just as at risk for a hardware failure or ransomware of any other number of things that can take them offline for days or permanently, because they didn't have effective backup. So just following the trends in the news may not be the best answer for businesses. They may need to get someone who understands their business to help them identify their risk profile and spend their money effectively, so their greatest risks are addressed first.

Obuchowski: There are a lot of services out there, but I would add a word of caution that everyone seems to be a cyber-security expert nowadays. You have law firms, IT companies. Everyone is jumping on the cyber-security bandwagon. So it's not so much about the services that are available as it is about the individual or company that is providing those services. Business need to vet qualifications, because some of them have just recently become self-proclaimed experts in the field.

Q: What are some of best practices to help monitor for and identify breaches?

Vincent: Even the most sophisticated companies often don't know about a breach until they are notified by a third party, such as law enforcement. While it is impossible to be sure you will identify all suspicious activity proactively, some key things to watch for are computers within your system that are behaving abnormally, users identifying suspicious emails, or unusual network traffic. Sometimes the first sign of an issue is a phone call from a user that has received an unusual email (and perhaps has already clicked on a link in that email or replied to the email). Other times, users may report that a computer or group of computers is operating particularly slowly or is generating unusual error messages or otherwise performing differently than usual. To the extent you have the ability to monitor traffic and activity on your network, review the logs. Signs of unusually high traffic in or out of the network, or traffic between parts of the system that don't typically communicate directly, can all be signs of malicious activity. It is important to investigate these types of occurrences, or if you have a vendor handling those issues for you, to make sure the vendor looks into the incidents.

Jackson: For small businesses, it's really a tough question. There are a lot of technologies available that can help them monitor their network, monitor file activity on their servers, and monitor traffic as it flows across their firewalls and various appliances. Some of those are very expensive and might not be affordable, but they do exist. There's data-loss prevention software that can read into data and determine if a social security number is outbound or if some type of data profile is sent across the network. Most of those services are going to be technology based. Some of it goes back to your employees as well. You have to educate them and make sure they're aware of what's going on in the environment, and to notice small details. Unfortunately, most breaches occur and they're not discovered for two to three weeks after it actually happens. And many times it's not a technical safeguard that catches it. In one notable event involving the Federal Reserve, what caught it was the person who was doing the fraud misspelled a word in an email request for the wire transfer. So there are a lot of technical aspects and best practices and technology implemented, but it goes back to employees. They need to be aware, they need to key on certain things. And if something looks out of place, they need to question it.

Powell: There was a horror movie I watched when I was growing up where this babysitter kept getting this threatening call. And then finally the police called and said, “The call is coming from inside the house.” And it turns out the guy who was calling was upstairs. I think a lot of times with these breaches, the call is coming from inside the house. There’s a disgruntled employee or a dumb user, and there’s no technology solution for a dumb user. I think we worry sometimes about somebody kicking in the door to our house, when we really need to worry about who we’re inviting in. Who do we willingly let in? That goes to a lot of different components about vendor management and the whole education piece. So I think a lot of the identification of it is just kind of understanding who your users are and what’s their typical profile.

Sawyer: Technology has come a long way, and some of the things are less expensive and less intrusive than they used to be. There are some basic measures, but it’s mainly the holistic approach. It’s understanding what your business is and what it does, and getting everybody involved. So if something is out of the ordinary, you probably should question it. The last thing you want is for the FBI to call and say you have a problem. Some of these internal breaches go on for years and aren’t found, even in big companies. So there’s a tendency to throw lots of tech at things, and the vendors love it. But a lot of it is a common-sense approach of understanding your business, finding out what makes sense and getting everybody involved. And if something is out of the ordinary, speak up.

Obuchowski: We’re talking about the B word – breaches – and we have to keep in mind that breaches are bad just because that term in and of itself carries the regulatory and legal impact with it. I’d rather say security incidents, because not every single incident is going to amount to the level of a data breach. There are some technologies out there for detecting incidents. From an investigation standpoint, the most valuable one that comes to us and to an organization are the logs. So you have what’s called your Sims, which basically is a correlation of log files to see what’s taking place on your network and being able to identify what systems are being accessed. The managed services of your firewall, your email, etc., will also help identify when things are occurring. You have to keep in mind that just because we’re in a technology world, it doesn’t mean that all these incidents are going to be in an electronic format. So it ties back to risk assessment – knowing what information you have – because you can suffer an incident in paper format. A lot of government, higher education and other businesses still store vast amounts of employee data or student data in that paper format. Those also have to be taken into account, because how do you detect somebody going into an unlocked office and stealing employee files from a file cabinet? So you have to keep in mind that not all these incidents are going to be in electronic format. Some of them can be in paper.

“Even the most sophisticated companies often don’t know about a breach until they are notified by a third party, such as law enforcement.”

- India E. Vincent

Asbury: The one crucial component as it relates to a best practice is to have at least one – and hopefully more – competent employee who understands risk management as it relates to IT. Role assignment is crucial, and that includes a competent security manager or information security officer who can implement processes and protocols to manage security and monitor for an incident or breach. There are also a lot of enterprise-grade technologies out there that are now available to businesses at an affordable price point. Things like intrusion detection and prevention services, web-content filtering services, and monitoring and logging components that are all included in what’s called next-generation firewalls. So for a reasonable price, an organization can invest in technology that will provide some alerting mechanism. And then I will again stress the importance of regularly checking on the health of an organization. Most organizations that experience a breach find out about it weeks or months after it happens. The best way to reduce the window of vulnerability is to regularly assess the degree of risk that an organization sustains.

Q: What are the key components to be included in a breach/incident response plan?

Obuchowski: The three things to look at are, first and foremost, that there is a central point of contact, whether it’s an email or a telephone number. What you don’t want to do is have employees try to handle the incident themselves. There needs to be a central receiving point for any type of incident. The next key component is having the response plan triaged, so you have some type of classification internally for that receiving point. You have a type 1 incident, type 2, type 3. The type of incident will trigger internally who to contact. Which leads to point number three, which is having that contact list. That will also include external vendors. For example, IT is not forensics. They work together, but there are two different objectives for that. So part of your response plan might be having outside vendors who are experts at handling different types of incidents, such as outside council for data privacy. Because what you don’t want to do is hire a divorce attorney to handle your data incident. They’re not going to be qualified because that’s not something they practice on a regular basis. So have a central point of contact, have a triage depending on the type of incident, and then have that contact list, which includes internal people and also external vendors.

Powell: Culturally in the businesses community, we need to be less judgmental of people who have breaches and incidents, because you’re next. If we all lived in the same neighborhood and somebody’s house was broken into, we’d have a community meeting to decide what happened and how we can better prevent this type of thing from happening again. There would be this kind of collective education that would come from that. There is still this embarrassment factor from having cyber-security incidents, and businesses don’t want to be public about it. Where I think there is a lot of benefit if people are willing to share the knowledge in that space. We can share what this threat really looks like, so as a business community there can be some education around that. So when incidents come out, I don’t think we need to have a shaming of somebody. The media takes a roll in that shaming, when really it should be, “What can we learn from this?”

Sawyer: If you’re having to ask this question, you probably need to be asking some other questions first. Because either you know the answer, or you should be calling somebody who knows the answer. There is a lot of sharing of information in Birmingham. If you join InfraGard or some of these other organizations, there is a lot of sharing of information about how we can protect each other. So developing a response plan is important. It’s important to know who to call and what your regulatory and legal requirements are. Every business should have a plan of at least the first three people they have to call to figure out what to do next.

Asbury: Start with engaging the right people in the development process. If the right people aren’t at the table when it’s being developed, then the plan itself is not going to be as effective. Through that development process, there should be a designated internal security manager or officer. I would also recommend the engagement of a qualified third-party organization that specializes in risk management and cyber-security. And then a critical element is to engage an attorney or law firm that specializes in incident risk management. Once there has been effective development, the other point to consider is role assignments. Who does what in the event of an incident? That doesn't always just include IT employees. Who responds in what way is something that has to be worked through. One thing to consider is to have a mock exercise – often called a table-top – which plays through the steps taken in the event of an incident. Afterwards, work through that and determine whether the execution of those plans is actually effective or needs modification.

Jackson: It really is an us-against-them mentality that we have to have. We all need to assume that we're going to get attacked, and we need to respond now and not wait until it actually happens. One of the ways we can respond is through better collaboration among groups of people. The more smart folks who get in a room, the better equipped we're going to be to handle any type of issue that comes up. You need to have a plan. There are websites and resources and all types of information out there on how to develop it. I'd put it almost in the same bucket as a disaster recovery plan, but it's a different type of disaster that's happened.

Vincent: First, specify the criteria that will be used to declare an incident or a breach, the individuals who are responsible for making that declaration, who will be informed of the declaration and how they will be notified. The incident response team should include an Incident Lead, a business decision maker, external legal counsel with expertise in data breach responses, external forensic specialists, and HR, and possibly law enforcement, an external PR firm or a data breach resolution provider. Each team member needs a copy of the incident response plan and contact information for all team members, in paper form, because you should not rely on communications via the compromised system. The response plan should include a checklist for the first 24 hours after declaring an incident or breach; a list of follow-up activities; a description of the hardware and software components of your system and expected data flows between these components; contact information for your identified third party vendors; and a list of customer/client notification requirements applicable to your business. In addition to responding to the breach, you need to identify who is going to focus on maintaining or restoring business operations, and what resources they will need to do so. Finally, make sure the incident response team practices implementing the plan in simulation exercises.

Q: What are some things businesses often overlook when developing a plan to protect their sensitive data?

Sawyer: If you look at the definition of personally identifiable information, the stuff that used to appear in the phonebook is today considered personally identifiable and shouldn't be freely distributed. So a lot of businesses have a lot of personally identifiable information. It's not just social security numbers. It's really any aggregation of information that organizations don't think about, but they have tons of that stuff lying around. We're talking mainly about cyber, but there are a lot of paper documents just lying around in businesses that many times gets overlooked. Stuff gets thrown in the trash, and dumpster diving is still a popular way to breach organizations. A lot of stuff gets loose that way. Another thing is encryption. Many people ignore that they are sending a lot of stuff in the clear in open emails. You should consider emails to be postcards. They're really not that hard to read. So a lot of those things get overlooked, and yet there are inexpensive and effective solutions for that today. The other thing that gets overlooked all the time is insurance. For small businesses, cyber insurance policies are really not terribly expensive. There are some good broad-form coverages out there for very small amounts of money, and that's some of the best money some small businesses will spend.

Obuchowski: How can you protect the information if you don't know what you have? It goes back to risk assessment and overlooking the types of information that is stored. First you need to know what you have in order to properly protect it.

"First you need to know what you have in order to properly protect it."

– Andy Obuchowski Jr.

Asbury: When these plans are being developed, there's often not enough engagement from key stakeholders who are part of the business process. It is important to have the right people who can bring the right information about how business is conducted after the attack. Organizations can't just rely on an IT manager who is solely focused on IT to bring all the necessary information to develop a really good and solid plan. Also, internal risk is often overlooked. There's often an assumption that the primary risk is outside the organization. However, the primary risk of incident involves data leaving the organization, even if it's unintentional. So the vulnerabilities themselves are more often than not internal, and it begins with our own employees. Oftentimes that's not really considered, but proper safeguards from within are critical. So it is important to ensure that employees are engaged in the process.

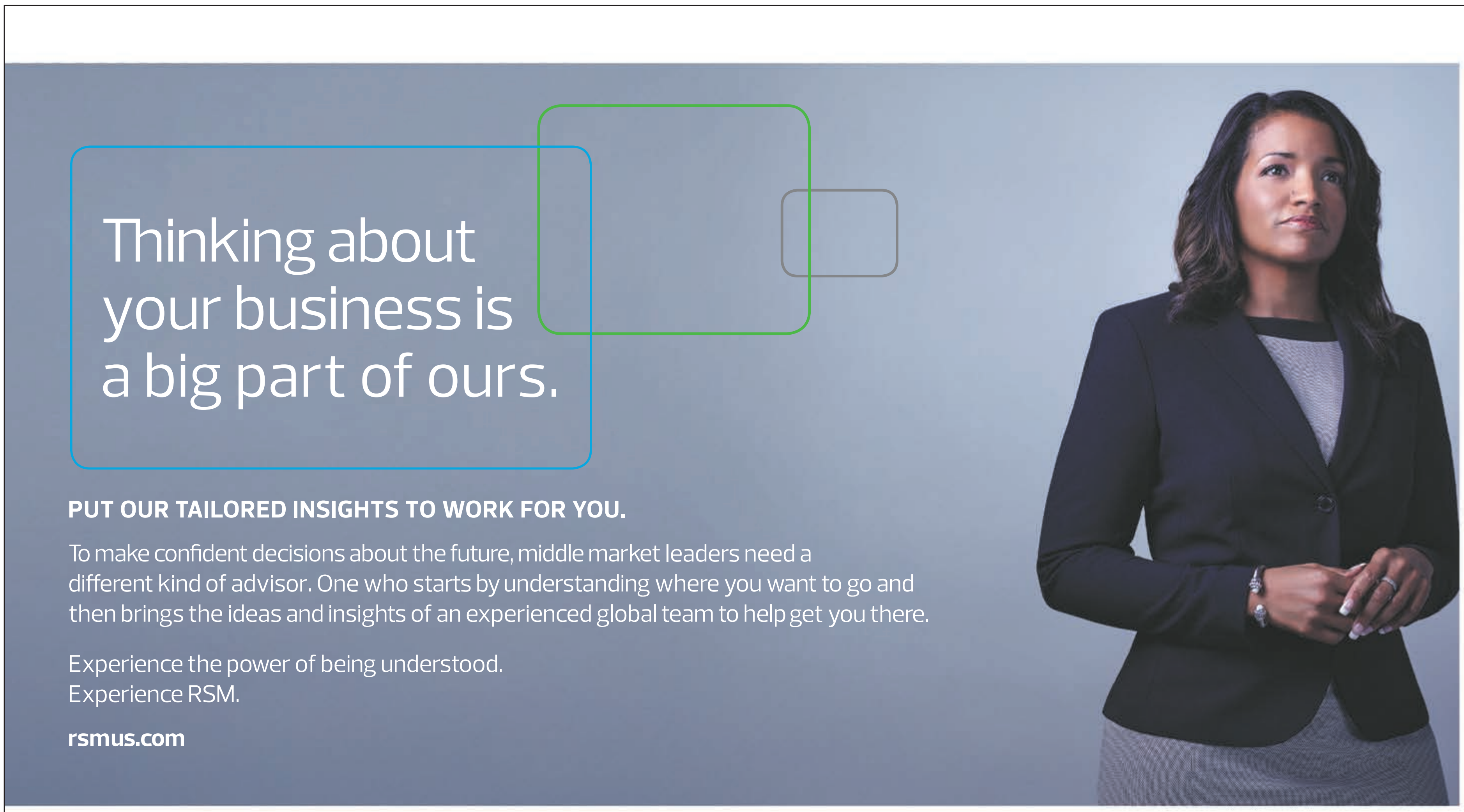
Jackson: I think one of the most overlooked threats is mobile devices. As devices have gotten advanced, they're able to store more data, and they're used every day to integrate into our businesses. They really span that gap between personal and business. We put aps on our phone that are mixed in with business data, and we don't always know the risk of mixing those two together. Plus, when you take a mobile device you can connect to hotspots and different Wi-Fi networks that are virtually anywhere. When you do that, you're not behind the safeguards of your corporate network. Also, these devices are basically storage devices. They can be used to offload data, and they properly wouldn't be suspected. If you carry a USB device into a company, it might look suspicious. But if I carry in my iPhone, it wouldn't look suspicious as a method of taking data out of an organization. So there needs to be a bigger focus on mobile devices and how they're secured, and make sure employees know the proper use of those in a business environment.

Vincent: I agree about mobile devices. People generally don't think about the computing power typically available on a mobile device or the amount of data that can be compromised if such a device is lost, stolen or hacked. Because society tends to rely on mobile devices for convenience both personally and professionally, users often want to compromise security of these devices for convenience. Businesses should always make an assessment between the business risk and convenience of their users, but it is important that the choices about mobile device security be well considered and not driven by the latest features available in technology. Possibilities to consider are password protection, two-factor authentication, encryption, ability to remote wipe a device, and lost device locator options.

Powell: It's important to know who has access to what. If you came to my home, I wouldn't give you the code to the gun safe. As companies grow, your accounts payable clerk may have had access to the shared network when there were 10 employees. Now that there are 500 employees, she may still have access to the S drive, but it now has a very different set of data in it than when they first started the business. So as businesses grow, you need to have a persistent review of what is the sensitive data, and who has access to it.

Q: What are some good components of an emergency plan as it pertains to cyber security and protecting/backing up data?

Obuchowski: The key component of backing up



data is testing your backups to make sure you can actually get into them. A lot of organizations just assume their backups are working properly, and they store them offsite or on another service. So you need to test your backups to make sure you can actually restore them and it contains the information you want to backup.

Asbury: Oftentimes, IT managers feel that if there are good backups, business continuity is assured. But if that process isn't tested on a regular basis, organizations are at risk. Second to good backups is the encryption of data as it relates to security management. And finally, a lot of organizations are now using outsourced solutions for offsite backups as part of their security plan. That's a great service, but I would encourage leaders to go through a proper vetting process to determine whether outsourced vendors are credible. Make sure they're storing your data in secured facilities that meet certain industry standards to ensure that your information is in fact secure, and that it is truly available in the event of an emergency.

Vincent: While it is technically possible to have systems that provide completely redundant, real-time business continuity, that is not cost effective for most businesses, particularly small to medium size businesses. Each business needs to consider the aspect of their business that would be critical to continued business operations in the event of a data incident, a natural disaster, or similar occurrence that makes the primary systems unavailable for some reason. The key is to identify those critical items, find ways to ensure they are available in a reasonable time through a secondary source, and to prioritize other systems and determine how you would go about retrieving that functionality and/or which vendors will handle this function for you.

Jackson: Having a reliable, tested backup is one of the most important components. But I also believe you have to have a mechanism and process in place that you monitor on a regular basis. Look at it and make sure it's running, make sure it's complete and it has the integrity needed for recovery. Because we're really taking about recovery, not just backing it up. So management monitoring of that process has to be a key component. Too many times we've asked clients when the last time their backup ran and they can't tell us because they don't look at it. They just assume it's running and then they find themselves 20 or 30 days behind, which puts them in a very bad situation.

Sawyer: Businesses have lots of different kinds of data and they're not all at the same importance level. Some types of data may need to be backed up in different ways than other types. Some may need to be more readily available. So a little bit of planning to understand all the data that is available in the business and how important it is to the business is really paramount to figuring out what's an appropriate methodology. The other thing we're seeing a lot is small businesses feel that they're backing up by using file synch-and-share solutions like Dropbox, iCloud etc. I'm afraid they're mistaken. For instance, if you get a CryptoLocker type virus, that's just a folder on your drive. It's going to get locked as well and you're going to lose your data that way. And some of the newer pieces of ransomware and other types of malware actually go out and look for online backups. Any kind of backup is better than none, but with a little bit of study and effort, you can end up with a really effective backup solution that is not terribly expensive for businesses.

> *"It's important to know who has access to what. If you came to my home, I wouldn't give you the code to the gun safe"*
>
> *- David Powell*

Q: What options are available to train employees about the importance of cyber security?

Asbury: Most training programs can be reapplied to a number of different industries. The internet is a good resource to find material for training your employees. Those training mechanisms are very important as well. Once you have the information put together, the process of training is important. Don't just train once and consider it done and not revisit. There has to be that continued approach of ensuring that users and employees are aware of certain protocols and procedures. At Warren Averett, we have at least two meetings a year where we pull all our employees together for an update, and we carve out 10 to 15 minutes for our information security officer to update everyone on what's taking place relative to security. In addition, we use an internal Intranet site, and updates and reminders are posted on a regular basis. There are also refreshers about our information security plan and protocols that we have our employees read and sign on a regular basis. All of these points are good ones to consider and can be easily applied to many different organizations.

Vincent: You can prepare basic training on your own with a little time on the Internet. The FTC, NIST and the SBA as well as several other sources all provide good materials for educating yourself and your employees about the risks for small businesses. For larger companies that have the resources, there are vendors who will conduct cyber awareness, planning and/or incident response training as well as provide follow-up assessments and testing. This is one area where there is no shortage of information, and any additional knowledge you can give your employees about how to avoid breaches can have a direct impact on your chances of catching an intrusion before there is any damage, or limiting the damage once an intrusion has occurred. In either case, your cyber legal counsel can assist in identifying training materials or providers and can often even provide the training assistance.

Jackson: It's very important for a company to get training that's applicable to their business. Their profile may be vastly different from others, so there may not be a one-size-fits-all training for organizations. The most important thing is the frequency of the training received. We're talking about evolving threats that change. Training that was done two or three years ago does not apply today. The threats are different, and the means of delivery to the user are different. Training has to be done on a regular basis.

Sawyer: We love to do training. We do a lot of that in the community. Much of it is generalized and open to the public. There's a lot of that available. But one of the best sources is somebody who knows the organization. Tailoring something to the specific organization and the needs of that business and exactly the way their business process works is really invaluable. Ideally, the folks they work with on a regular basis for their managed services or other consulting services would be in a good position to understand their business and help them develop training that would be applicable and be of great benefit. But there is certainly a wealth of information out there, and everyone should look for it.

Obuchowski: The key point with security awareness training – just like with your incident response plan – is once you have something you want to test it. So it's a similar model. First and foremost, security awareness training should be ongoing, not just one time a year. Even something as simple as information flyers posted in a breakroom to remind people, or emails giving some generalized information but on an ongoing basis. That's the key thing with security awareness training. The other thing is to test your training. Just because you did the training, how do you know it was delivered effectively? So some other services out there are more on the social engineering side. Sending emails to a handful of people to see if somebody clicks on a link, and then reporting that back to the organization, so maybe they can reassess their training.