

TABLE of EXPERTS Series



INSIGHTS INTO:
CYBERSECURITY

Sponsored by:



S.S. NESBITT

TEKLINKS



ThreatAdvice
Assess. Educate. Insure.

Warren
Averett
TECHNOLOGY GROUP

THE EXPERTS



Jeff Bohman, CNA, CISSP | Vice President Managed Services, Warren Averett Technology Group

Jeff Bohman is a Certified Information System Security Professional and a Certified Network Analyst with more than 30 years of experience and technical training in a variety of industry leading hardware platforms and operating systems. Jeff has a strong background in Security and Compliance, and oversees technical, project and data center services for the Warren Averett Technology Group. Before joining Warren Averett Technology Group, he was a Regional Technical Specialist for a Fortune 100 Manufacturer; served in Customer Engineering Services and Management roles supporting State and Federal Government, as well as commercial clients; held an executive leadership position with responsibilities involving technical consulting, service, sales and vendor management.



Will Enochs | Co-lead of Cybersecurity Consulting Group, TekLinks

Will Enochs co-leads TekLinks' Cybersecurity Consulting Group. He boasts over 15 years of deep technical experience spanning multiple IT disciplines. In addition to performing a wide range of technical and non-technical cybersecurity engagements, Will is responsible for the growth of the cybersecurity practice – including go-to-market strategy, and technical development of TekLinks' cybersecurity portfolio.



Mike Roman, CRM, CIC | Vice President Property and Casualty, S.S. Nesbitt

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 as vice president of Property & Casualty at S.S. Nesbitt (SSN), an independent insurance agency and division of ESBCO Industries, Inc. Mike is a member of the agency's leadership team, overseeing the daily operations of SSN's Property & Casualty department. Prior to his work in insurance, he was a pilot with American Airlines after a distinguished career as a Naval Aviator with the U.S. Navy. He is a graduate of the Virginia Military Institute.



Jennifer H. Skjellum | Director of Blockchain & Crypto Innovation, ThreatAdvice, LLC

Jennifer Skjellum is the Director of Blockchain and Crypto Innovation for ThreatAdvice, LLC. ThreatAdvice provides cybersecurity education, awareness, prevention and threat analysis products and services aimed at helping business protect themselves from cyber intrusions. Skjellum's career includes experience building companies, building educational programs for undergraduates and professionals, and nonprofit organization leadership. In addition to co-founding the region's largest cybersecurity conference- Alabama Cyber Now, she is well versed in the world of scalable, open systems including high performance computing, scale-out data centers for big data, and grid/cloud computing infrastructure from experience spanning over 25 years in industry leadership roles.

Q: It seems like the past year was filled with cyber breaches. Just how big of a risk is cybersecurity for small businesses, and is the risk increasing?

Jennifer Skjellum: Every business, regardless of size or sector, needs to be vigilant about preparing themselves for cyber intrusions. Cyber risks are ranked as the most underestimated threats to businesses, but come with the most long-term negative impact. Cyber incidents continue to clearly show an upward trend. For example, five years ago, cyber incidents ranked number 15 in an EY study. In the 2018 list it increased to number two. Recent events such as the WannaCry and Petya ransomware attacks brought significant financial losses to many businesses. On an individual level, recently identified security flaws in computer chips in nearly every modern device reveal the cyber vulnerability of modern societies. And the potential for so-called cyber hurricane events to occur – where hackers disrupt larger numbers of companies by targeting common infrastructure dependencies – will continue to grow in 2018.

Mike Roman: Big-name breaches such as Home Depot or Target are exciting and attract media. In contrast, breaches

experienced by smaller companies often fly below the radar. When you compare the number of attacks on large companies versus smaller companies, the numbers may surprise you. About half of all cyber attacks target small to mid-size businesses. Unfortunately, smaller companies will likely experience a much greater impact since they have fewer resources and less financial ability to handle an attack. This risk is increasing at an alarming rate. Some reports indicate that the volume of cyber attacks nearly doubled in the first half of 2017.

Jeff Bohman: The Center for Internet Security Multi-State Internet Sharing and Analysis Center identified a record-setting number of data breaches in 2017, surpassing the previous record year of 2012 by 18 percent. In the fourth quarter, there was an 80 percent increase in the quantity of reported breaches when compared to the third quarter. While small businesses may not seem as attractive as large corporations, they are usually easier to compromise and are increasingly targeted. According to Symantec's 2016 Internet Security Threat Report, 43 percent of cyber attacks target small businesses. This is a dramatic jump since 2011, when this figure was only 18

percent.

Will Enochs: All companies/computers connected to the internet are at risk of compromise, and I would say that in a general sense that risk is increasing. Cybersecurity, or lack thereof, is a formidable risk for every business that has computers connected to the internet. It is important to understand that the risk landscape is always changing in response to technology, and cyber-criminals are always working to leverage this technology to make money. If you take blockchain and cryptocurrency as a new technology, then you can see ICOs (Initial Coin Offerings) as a way to exploit these things. Unless you are talking about nation-state level actors, it doesn't really get much more complicated than that. Now that we have established that as a baseline, I think the amount of risk that a business faces can be directly correlated to their action or inaction as it pertains to identifying and responding to the threats facing their business. Companies that choose to do nothing while the threat landscape is changing will find themselves with substantially more risk as a result.

Q: If my company is the victim of a cyber attack, what are some of the

different ways it could impact my company?

Roman: Certainly the most negative impact will be a reduction in your revenue. You will lose money. When you suffer a breach of protected information, you will likely have to comply with state and/or federal laws, and you will need to hire vendors to handle different aspects of the breach. The types of vendors you will need by your side include forensics, legal, credit monitoring, and crisis management. Many companies overlook the fact that they will expend significant internal resources while handling a breach. The cost of these internal resources is difficult to quantify and will not be covered by insurance. Potentially, one of the most devastating impacts will be damage to your reputation with your clients and customers. A poorly handled breach could result in lost revenue for years going forward.

Bohman: There are both direct and indirect costs incurred by victims of cyber attacks. Businesses affected by a cyber breach will face indirect investigation and recovery costs, and direct costs can include theft of financial information, such as bank or payment card data. Reputational damage resulting from a cyber breach can lead to loss of sales,

loss of existing customers and reduced profitability. Regulatory consequences of a cyber breach can also include fines and sanctions, notification expenses, restitution costs, contractual/vendor agreement obligations and legal expenses.

Enochs: Companies that suffer from a substantial cybersecurity incident usually start with a stream of negative impacts that can be put into three broad categories: operational, financial, and reputational. While sometimes hard to quantify, all these categories usually have their own correlating financial impact that range from the loss of data and productivity to the loss of customers and regulatory fines. Fortunately, after the negative impacts have passed, the best and most lasting impact is hopefully an investment into increased data security and network visibility for the benefit of both the company and its customers. The latter are the outcomes that I get the most excited about, and should your company experience a show-stopping cybersecurity incident I hope you don't miss out on the positive outcomes on the other side of the tunnel.

Skjellum: Loss of reputation, customers, data, intellectual property and revenue are all potential side effects of a cyber attack. Disruption of services, such as email and

phone, could impact normal business operations for hours and even days. Almost 50 percent of small businesses have experienced a cyber attack, and as much as 60 percent of small and medium-sized businesses who are hacked go out of business after six months.

Q: How can my company reduce the likelihood of a breach?

Bohman: Proactive and preventive measures are more important than ever to maintain the health and security of your information technology. Before shelling out for the latest techy/niche solution, address prevention. Prevention is 99 percent of the solution. Massive breaches are all preventable, and adhering to the following tips will eliminate most threats. Replace and patch obsolete hardware and operating systems; upgrade and patch your applications; verify patch and configuration vulnerabilities through routine scanning; secure physical and logical points of entry; implement hardened security baselines; and enforce

strong passwords and access procedures.

Enochs: This is such a personalized question based on how the company operates, but some general words of wisdom aside from doing the basic IT functions well – patching, vulnerability scanning, baseline operating system hardening, etc. – would be to choose a risk management framework such as the Internet Security Top 20 Controls. Or, if you are more mature in your security program, the

NIST Cybersecurity Framework. Once you begin to view cybersecurity through the lens of quantifying risk and making decisions from there you will be much better off.

Skjellum: The number one thing all companies need to do is provide security awareness training for employees. In addition to making sure all employees are aware of the common techniques used by cyber criminals, companies need to provide and enforce guidelines, policies and procedures for digital communication, data transmissions and general internet

use.

Roman: Talk to people who are familiar with cyber exposure. Speak with your internal or outside legal counsel, your CPA firm, other companies and your insurance advisor. Stay ahead by gathering information. Business periodicals report often on cyber exposure and ways to mitigate and reduce your chances of an event. Develop a game plan. Meet internally within your organization to implement proactive changes to address cyber risks before a breach. Also, this is not a one-and-done event. Your internal committee should meet quarterly to address new cyber threats and complimentary changes to your program.

Q: How can I choose a professional firm to help protect my business from cyber threats?

Enochs: The first thing you have to understand is the answer to this question requires at least two different groups of experts with complimentary but usually different skillsets. Simply put, people who are good at defense and people who are good at offense. This could be the same firm, but it will undoubtedly be different people or groups within the firm. Because misconfigured and mismanaged systems account for a very

“Many companies overlook the fact that they will expend significant internal resources while handling a breach.”

-Mike Roman

THERE ARE THOSE WHO HAVE BEEN HACKED AND THOSE WHO WILL BE



GET BACK TO BUSINESS FASTER

CONSULT OUR CYBER INSURANCE EXPERT

Mike Roman, CIC, CRM
Cyber@ssnesbitt.com

S S NESBITT

AN EBS CO COMPANY

Fortune 1000 know-how for Alabama's small to midsize companies

large portion of vulnerabilities I see on a day-to-day basis, you will be best served to hire someone who is an expert at the hardware/software you use or let the person you hire choose their own tools. There are always exceptions, but remember the main goal is to have well managed, correctly configured, up-to-date hardware/software. Secondly, you want to find offensive practitioners who can put your assets and their configurations to the test and subsequently provide you a detailed, well written, easy to understand report. You must not overlook the value of a good report as it is the only thing you will be left with after the engagement is over. You will also want to choose a partner that can understand your business and draw a straight line between discovered vulnerabilities and the impact it could have on your business.

Skjellum: Look for cybersecurity partners that go beyond just advising/consulting, and for those who provide services to both protect your organization against cyber threats and help ensure that your company's protection is well-rounded. Most companies will engage with several providers in order to ensure they have full coverage through cyber education, a sound and secure IT infrastructure and cyber insurance.

Roman: Selecting a professional firm to handle the various aspects of protection from cyber events can be challenging, especially for small to mid-size businesses. Start by speaking with members of your industry and community to find out how they have addressed this challenge, and how they went about selecting partners. Referrals from other companies whom you trust are vital. Or connect within your industry association for law firms, accountants, insurance brokers and IT firms.

Bohman: When searching for a firm, it's important to do your research. Ask the firms you are considering to provide examples of their proven experience. Have they been in the trenches and successfully remediated breaches? Do they have hands-on experience with current leading technologies? Do they have recognized technical, professional and security credentials? Do they understand your business? What security solutions do they use and service? What vendors do they have direct relationships with? What audits are performed on their own company? Do they do self-assessments or bring in a third-party? What are their standards? Asking these questions will provide insight into which firm is the best fit for your needs, and allow you to make an informed decision for your business.

Q: What can my business do to help educate my employees in an effort to boost our overall cybersecurity?

Roman: First, do not wait. Spend the time now to develop a short briefing regarding phishing attempts and other social-engineering fraud attempts. Organize a time to meet with employees and increase their cyber-threat awareness. Advise them not to click on any links in emails, unless they are positive that the email has come from a confirmed business partner. If you have an internal committee to address cyber exposures, then create a subcommittee devoted to increasing employee awareness, training and education. Consider partnering with professional firms who can help educate your workforce and implement tools to test your employees' level of cyber awareness. For example, many IT security firms are able to send artificial phishing attempt emails to employees to see if they respond. If they do respond, the employee can be given further training to elevate their knowledge.

Bohman: Implement a formal IT security awareness training. Feature an initial introductory session at each new hire orientation for incoming employees, and host a refresher training for all employees annually, at minimum. Also, consider implementing email security training to test and educate users on how to recognize malicious emails and social engineering/phishing attacks. For supplementary cyber education, subscribe to security reporting services to keep informed of current events, new regulations and technical advances so you and your team can stay knowledgeable between training sessions and updates

Skjellum: Train your employees to recognize common cybercrime and information security risks, including social engineering, online fraud, phishing and web-browsing risks. Provide guidelines for creating strong passwords that cannot be easily guessed, but can be remembered. Make sure your employees are aware of the dangers of clicking on emailed or online links that are suspicious or from unknown sources by reinforcing that even the simple act of clicking on a suspicious link or attachment can release malicious software, or worse, infect computers and steal company data.

Enochs: Not only should employees have the right amount of knowledge, but actually implement the knowledge as well. To enact change in any organization, you must have buy-in from the top of the org chart. That means compliance with the company's policy and commitment to devote resources to the initiatives. Having a necessary-evil or check-the-

box mentality is never going to elicit employee buy-in to the idea that they play a valuable part in the overall security. Their understanding of this will also help temper some of the inevitable changes that will need to happen but inevitably make certain tasks take longer. Everyone would agree that it takes longer to lock your doors than it does to leave them unlocked. Most people consider the trade-off worth it. One example of a business function that takes about as long is approving a 2FA push notification. It's not much time, but if you value security it is worth it in the end.

Q: What are some of the key ways cyber attacks happen (i.e., points of vulnerability)?

Bohman: Some recent and highly publicized breaches provide examples of common vulnerabilities that left companies susceptible to cyber attacks. These misfortunes of other businesses are warnings your business can heed:

- For Equifax, an unpatched open source web application development software compromised the personal identity information of 143 million consumers. Vulnerability scanning, remediation, and patch management failure.

- In separate incidents, Uber exposed sensitive development information on an external collaboration site, GitHub, in successive years. This affected 57 million individuals, and management colluded at the highest levels to cover up this blunder. Data identification and management practices failure.

- Dun & Bradstreet sold a database to thousands of companies and subsequently found its marketing database, containing over 33 million corporate and government contacts, shared across the web. Accidental exposure, poor third-party controls.

- Deloitte failed to employ two-factor authentication, which would have prevented an administrative email account from being hacked. The result was compromised email data and address lists, including Deloitte's biggest clients of primary interest. Access management and audit procedure failure.

- A breach originated in 2014 at Yahoo from a spear-fishing email and weak passwords. Four people were indicted by the FBI in March of 2017. Two of the four were Russian spies who were charged with the hack, which compromised more than 3 billion accounts. Training weakness. Applications not whitelisted.

Skjellum: The two most common attacks are malware and phishing. Criminals have evolved and the attacks

have become more sophisticated, but they are still largely successful due to human error. Attackers will use a variety of methods to get malware into your computer, but at some stage it often requires the user taking an action to install the malware. This can include clicking a link to download a file or opening an attachment that may look harmless – like a Word document or PDF attachment – but actually has a malware installer hidden within. In a phishing attack, an attacker may send you an email that appears to be from someone you trust, like your boss or a company you do business with. The email will seem legitimate, and it will have some urgency to it, such as fraudulent activity has been detected on your account. In the email, there will be an attachment to open or a link to click. Upon opening the malicious attachment, malware will be installed on your computer. If you click the link, it may send you to a legitimate-looking website that asks for you to log in to access an important file, but the website is actually a trap used to capture log-in credentials. In order to combat phishing attempts, understanding the importance of verifying email senders and attachments/links is essential.

Enochs: There are two big buckets here that are equally as dangerous. The first bucket is technical, which would include all your technology assets, whether on premise or cloud. The most common vulnerabilities in this area are devices that are affected by a publicly known exploit, have been misconfigured, or are utilizing weak configurations. Some examples of this are old unpatched perimeter devices like firewalls and even more common are vulnerable – and sometimes forgotten – web servers that are exposed to the internet. The second bucket is social vulnerabilities such as employees choosing very weak or common passwords that are easily guessed. And finally, the susceptibility of employees to phishing emails is the most common and usually the most effective technique at gaining access to company systems or data.

Roman: Currently, the top two cyber attacks are ransomware and social-engineering fraud. With ransomware, your information – or your customers' information – is quarantined by a hacker until you pay the hacker to release your information. Ransomware is very often presented in the form of a demand for Bitcoins, an electronic currency recognized worldwide. These ransomware attacks can be difficult to prevent. When they do occur, companies often go into panic mode. If you have insurance for cyber

events, I recommend that you contact your broker immediately so they can connect you with your breach coach to help guide you through your event. Social-engineering fraud is where an employee is tricked into divulging bank account or computer system information. This is a significant threat from a frequency standpoint. It is critical to note that social-engineering fraud is usually not covered by your more common insurance policies. The good news is that insurers are beginning to provide some insurance coverage for social-engineering fraud events within stand-alone cyber and crime policies. Make sure you and your insurance consultant know your policy coverages.

Q: We are a small company with limited IT expertise and resources. How do we protect ourselves?

Skjellum: There are the five key areas that every company, regardless of size, needs to be vigilant about. First, educate your employees. They are your first line of defense, and education can go a long way in helping them help you protect your company. Develop a security policy. Keep your hardware, software, and security safeguards up-to-date. Strictly enforce

password policies for your employees and all business accounts. And evaluate cyber insurance policies

Enochs: First, you have to make it a priority and link information security to business objectives. It might seem unrelated, but without this first step, the resources of time and money will never be allocated. There is a very robust open-source community in the information security space, but you will have to make the time investment. The days are coming where companies will not be able to exist without the IT expertise. Just as is the case will all vital aspects of the business you can grow the expertise internally, hire the expertise or outsource the expertise, but you cannot exist without it.

Roman: The smaller the company, the less financial resources you have to handle cyber risks. Consider contracting with an outsourced IT firm, at least for some consulting. If you can't afford to hire an outside firm to manage your

programs and software, then at least have the firm provide guidance, which won't tax your cash flow quite as much.

Spend time educating your workforce and reviewing or implementing controls and procedures to limit your cyber exposure. These activities will be less costly but can help you avoid cyber breaches. Purchase insurance coverage for cyber events. More and more insurers are providing cyber coverage, which means cyber insurance costs are competitive. It's a buyer's market. However, not all cyber policies are necessarily appropriate for your risk. Look for an

insurance partner with an experienced cyber insurance professional on their team to ensure you are appropriately covered.

Bohman: The threat of a cybersecurity breach can be intimidating for a small company, so it's important to begin with the basics and discover what is most needed by your individual organization. Start by self-assessing and reviewing documentation in place for your current

personnel, systems, processes and procedures. Once you have established where your current position is regarding cybersecurity, engage outsourced expertise to help you perform a gap analysis and employ strategic planning. Overall, for basic security measures, common steps are to implement hosted solutions – such as Office 365 – for email, and outsourced services such as SIEM log correlation. You may discover that it would be helpful to engage outsourced expertise to assist with implementations, like CIS hardened security baselines or encryption.

Q: If my company has been breached, what are some key steps to respond?

Enochs: The first step is always to follow the steps outlined in your incident response plan. Failure to prepare and being forced to respond in a reactive manner is never a good place to find yourself. The TekLinks Cybersecurity Consulting Group uses the non-original Predict, Prevent, Detect, Respond, Recover, Improve workflow. If you find yourself with your hair on fire trying to respond and recover, you should probably enlist the help of a trusted partner. Furthermore, don't forget about consulting your lawyer and ensuring you

“Loss of reputation, customers, data, intellectual property and revenue are all potential side effects of a cyber attack.”

-Jennifer H. Skjellum

**DON'T BE ANOTHER STATISTIC
START YOUR CYBER EDUCATION TODAY**

ThreatAdvice is a cybersecurity awareness training platform that analyzes your business' risk environment, educates your employees, and performs awareness exercises and simulations so that you AND YOUR TEAM will always be cyber prepared.

WHAT'S INCLUDED

- Cyber News / Alerts / Updates
- Self Assessment Tools
- Policies & Procedures
- Awareness Campaigns
- Cybersecurity Best Practices
- Cyber Insurance Review
- Library of Course Overviews
- Learning Management System
- CyberStar / Hotline
- Phishing Simulation
- Risk Analysis

CALL 800.915.3381 TO GET STARTED TODAY

Visit our website at threatadvice.com for a detailed list of services included.

ThreatAdvice
threatadvice.com | info@threatadvice.com

follow any order of operations that is listed on your cyber-liability policy if you think you might have to submit a claim.

Roman: Before you call your attorney, call your insurance broker. This can't be stressed enough. You need to comply with the terms and conditions of your cyber policy, or else you may jeopardize your insurance coverage. There's a good chance your cyber insurer has already vetted vendors that they will organize at a moment's notice to walk you through your breach. Also, you will likely have one point of contact – a breach coach – to help you through the process. Your breach coach will be invaluable. In fact, access to a breach coach is arguably the most important reason a small to mid-sized company should purchase a cyber policy. If you experience a breach and do not have cyber insurance coverage, reach out to your legal team to begin the process. The two most urgent issues you will need to address are the extent of the breach and the laws with which you will need to comply in order to notify potentially affected individuals. Most larger law firms have attorneys experienced in cybersecurity events.

Bohman: Follow the steps outlined in your incident response plan. This should

include coordinating with your outsourced IT services and documenting the breach by logging actions into a ticketing system.

Complete and retain your incident response form and checklist for your records. Then, initiate containment and a preliminary assessment of the breach and its impact on your company. Evaluate the risks associated with the breach to determine what other steps are immediately necessary.

Skjellum: Once your company becomes aware that a breach has occurred, technical personnel and business decision-makers should work together to decide on the most practical and effective containment plan. After a containment plan has been established and execution has begun, get started on eradication and recovery efforts. Depending on the type of breach and type of business, your company may be required to notify local law enforcement or other government authorities upon discovery of a data breach. Many companies hesitate to contact the FBI or report the breach to authorities out of embarrassment, but the more data they have about cyber attacks, the more equipped they are to help. In the case of a ransomware attack, you should contact your local FBI office

or the Internet Crime Complaint Center to file a complaint online. In the event of exposure of customer information, you should notify the customers of the incident, record the data that was lost or exposed and record the measures taken to ensure against future exposure. Lastly, your company should always perform a lessons-learned meeting after the recovery phase has been successfully completed to discover, document and refine the knowledge gained during the incident handling process.

Q: My company has neglected its cybersecurity needs. What steps should we take?

Bohman: For small and medium-size businesses focused on a core mission and profitability, establishing a formal cybersecurity program can be daunting, so many companies elect to outsource their technical services. Many providers are expanding their services to include IT security services. Priorities for a cybersecurity program include: taking inventory of your company's assets (contracts, communications services, people, trade vendors, etc.); assessing your general

IT risks and vulnerabilities; prioritizing strategic planning; formulating or documenting a system security plan and a plan of action and milestones specific to your organization; and implementing controls and training your employees to be aware of cyber threats and how to appropriately respond to them. Once these preliminary steps have been taken, it's important to continually review, revise and reassess your cybersecurity needs. Your company is always changing and so is cybersecurity, so keeping abreast of updates in both areas will be beneficial for your business.

Skjellum: The first step is to complete a thorough cybersecurity threat assessment using credible professionals, who will provide an assessment for free. Once you have an understanding of what your company is lacking, then you can start with the basics.

Roman: First, form an internal committee to address the issue and arrange training for your employees. Develop a specific plan with your internal IT or external IT provider. Consult with similar companies or those people within your network who have experience in developing cybersecurity programs. Contact your insurance broker. Often,

insurance brokers experienced in cyber events will already have relationships with law firms and IT security teams, and they can guide you or connect you to them. An experienced broker can also help you understand the benefits of cyber insurance policies.

Enochs: Make it a priority at the C-Level and align security initiatives with business objectives. Perform some baseline gap assessment to identify where you are and where you want to be. Find a good consulting partner or make some strategic hires to get on the right track. Don't set goals that are too lofty but rather focus on some quick wins to show forward progress. Take one step at a time based on the prioritized results of your initial gap assessment and continue to reevaluate.

Q: What are some critical, but often overlooked aspects of cybersecurity?

Skjellum: Not offering cybersecurity training. How can you expect employees to prevent threats if you are not teaching them how? According to leading industry and government reports, 90 percent of all cyber breaches occur because an employee was not educated on the basic steps of cybersecurity.

Outdated software is also a problem. From apps to operating systems, software companies release updates that help prevent against the most recent data threats, but many companies don't have the IT staff to monitor and update their systems. Lack of awareness of current threats is an issue. For example, if you haven't heard of ransomware, then you might not be in the know regarding other new and noteworthy cyber threats. And finally, working over public wifi. We all love free wifi at places like coffee shops, malls and hotels, but are you aware of the security risks that you may be subjecting yourself to?

Roman: Unfortunately, the most prevalent overlooked aspect of cybersecurity is the lack of a cyber insurance policy. Too often companies believe that a top-notch IT program makes them impenetrable, and therefore they don't need to spend money on cyber insurance. Yet even if your security program is great, employees make mistakes or worse, act illegally and cause a breach. And you can still experience the old-fashioned breach in the form of hard-copy paper. Your first line of defense for cybersecurity is your IT protocol and procedures for preventing an event. But

“One attack trend that appears to be steadily on the rise is what most people refer to as supply-chain attacks.”

-Will Enoch

PROTECT YOUR DATA EVERYWHERE

TekLinks can help you protect your workloads everywhere you have data with software-defined and cloud-enabled Dell EMC Data Protection, including advanced automation and deep VMware integration.

Contact us today to learn how we can help you modernize your environment, automate tasks to simplify management and reduce costs, and transform to a software-defined and cloud centric data center.

DELLEMC **TEKLINKS**[®]
We Make IT Work for Business.



Alabama • Florida • Mississippi • Tennessee

205.314.6600 | teklinks.com

should the unfortunate happen and your program fails, a solid risk-transfer program to back it up is crucial to recovering financially and continuing your business.

Enochs: One thing I see quite often, even among companies that have prioritized security, is a lack of visibility into their third-party vendors and what their security controls are.

Bohman: The most commonly neglected areas include weak passwords and access controls, a lack of multi-factor authentication, inadequate network and system segmentation, insufficient baseline hardening, missing logs, limited recovery capability, poorly defined roles and responsibilities, improperly identified or positioned data, poor documentation concerning policies and procedures, and an overall disregard for security practices. Training, encryption and whitelisting of applications are also often overlooked. Assessed companies have competitive advantages. Until you have evaluated your business's stance and know what your specific organization's gaps are regarding cybersecurity, it is difficult to address your weaknesses.

Q: What are some of the top trends to be aware of for cybersecurity?

Roman: Ransomware has definitely

earned the top spot for the hottest current trend in cybersecurity events. It appears too easy for hackers to penetrate your

system to a level where they get to sensitive information.

And even though that information may be encrypted, they are very good at preventing you from accessing that information.

Bitcoins are a hacker's best friend, used to instantly and anonymously transfer money anywhere around the world. As such, ransomware has become almost a cost of doing business. Somewhere, the hackers must have an annual convention to set out maximum thresholds for the amount they demand for ransom, because in most cases the amount they are asking for is simply too easy for a company to pay, rather than investigate and attempt to find and prosecute the hackers.

Enochs: One attack trend that appears to be steadily on the rise is what most

people refer to as supply-chain attacks. Just like any smart businessman or woman, the cybercriminals are looking for

return on investment. The ability to compromise one software/hardware vendor that is used by millions provides that opportunity. Google Chrome extensions, WordPress Plugins and even the popular software CCleaner are great recent examples of this attack methodology at work.

Bohman: Things on the cybersecurity horizon include

an increased regulatory burden, the utilization of artificial intelligence and machine learning to boost cyber defenses, and the rise of botnets, which are used in brute-force hacking to identify new vulnerabilities and to withdraw stolen information. Phishing continues to be a top threat, and ransomware spotlights the importance of consistent and reliable backup and the benefits of application

whitelisting. Another key cybersecurity topic is sure to be the shortage of enterprise technical skills and expertise in the field.

Skjellum: Fraudulent instruction scams, when criminals use hacking and phishing techniques to accumulate information that allows them to send plausible-looking requests to transfer funds to bogus account, are in the rise. Fraudulent instruction incidents quadrupled in 2017, with the top three industry sectors affected being professional services, financial services and retail. Mobile device malware and ransomware are on the rise. Last year, mobile ransomware grew by over 400 percent. And with an increase in fake apps, adware and other mobile attacks, cell phones are no longer without risks. Cryptocurrency-mining malware also is on the rise. In February, security researchers discovered that at least 50,000 websites were quietly running crypto-jacking scripts allowing them to hijack the CPU resources of site visitors. Browser extensions that are specifically designed to block popular crypto miners from using your computing power are available for Chrome, and Firefox. Users can also add blocked domains to their ad blockers.

“The threat of a cybersecurity breach can be intimidating for a small company, so it's important to begin with the basics and discover what is most needed by your individual organization.”

-Jeff Bohman



Pictured: Paul Perry, Jason Asbury and Amy Walker

TECHNOLOGY AND RISK SOLUTIONS TO HELP YOUR BUSINESS THRIVE

Whether you are looking to meet needs in IT security, business software, risk and compliance, system infrastructure, or staffing and help desk, Warren Averett Technology Group can help you accomplish your goals. It's time to take a closer look at Warren Averett and all we have to offer.

Let's Thrive Together.



- TRADITIONAL ACCOUNTING 
- CORPORATE ADVISORY SERVICES 
- TECHNOLOGY AND RISK SOLUTIONS 
- HR SOLUTIONS 
- FINANCE TEAM SUPPORT 
- PERSONAL SERVICES 