Sponsored Content

THOUGHT LEADERSHIP SERIES

Technology & Cybersecurity

Tech success requires playing offense and defense

STEPHEN DAUGHERTY
Director of Technology
Sondhi Solutions
sdaugherty@sondhisolutions.com

ANDY MILLER, PH.D.
VP for Innovation & Partnerships
Indiana Wesleyan University
andy.miller2@indwes.edu

IVAN SHEFRIN
Executive Director
Managed Security Services
Comcast Business
ivan_shefrin@comcast.com

In our Thought Leadership Roundtable, leaders at Comcast Business, Indiana Wesleyan University and Sondhi Solutions cover the waterfront, from protecting your business from cybercriminals to making sure you're taking advantage of the latest technology.

Q: Cybercrime is on the rise and can be especially devastating to small businesses. How should businesses that are poorly protected or unprotected start the process of securing their assets?

Stephen Daugherty: There are two things small businesses can do today to protect their assets. The first is to ensure that their employees are trained to effectively identify potential attacks. This can be accomplished by implementing a Security Awareness Program. I cannot stress enough how employees are the front line of defense from hackers. Keeping them up to speed on the latest trends could save your business. The second is to ensure you have a sound backup policy. With a proper backup procedure in place, you will be able to recover your data no matter what.

Andy Miller: Though cybercrime can occur on a large scale, it often starts at the rudimentary level of security hygiene. Email phishing is a prevalent intrusion method, allowing bad actors to access critical information and create additional attacks. Weak password policies, absence of two-factor authentication (2FA), and sloppy access control protocols expose individual accounts. Small businesses should not sacrifice the security of their assets and operation based on limited resources. Security hygiene is a relatively inexpensive approach to securing one's information systems. Strong password policies, credential aging, required 2FA, and segmenting access to "need-to-know" accounts are relatively simple and inexpensive security measures. Ultimately, all employees must understand that security is everyone's responsibility.

Ivan Shefrin: Cybersecurity is a journey, not a destination. Buying the latest tools won't help without implementing controls around people and processes. Businesses of any size should put in place a security program to identify their most critical data and IT assets. We can't protect what we can't see. Then develop a plan to secure your crown jewel data first, which should start with backing up your data every day. Users are often the weakest link. Create a program to train your users, implement a strong password vault to improve credential controls, and use multi-factor authentication wherever possible. Scan for vulnerabilities and patch your systems. People work from anywhere now, including unsecured networks. Implement a remote access platform and policy to enforce security when people work from home, at least when accessing corporate data.

Q: What specific products are out there to help defend against attacks?

Ivan Shefrin: Products are important, but it is just as important to train your people and define some processes to help with business continuity. How would you react in the event of a cybersecurity incident? Would you know who to call inside or outside your organization, especially if you do not have access to your computer? Do you understand how to recover your data and does your team practice disaster recovery?

Once you have a plan in place, and you are comfortable with a level of risk appropriate to your business, then it's time to think about specific products to support your plan. Generally, you want to invest in products that help protect your most critical data first. Depending on the risks to your organization, it may not make sense to buy the latest shiny technology. There are some basic products everyone should think about, including next-generation endpoint protection, unified threat management firewalls, a password vault, multi-factor authentication, remote access security, and data backup and recovery.

Stephen Daugherty: Attacks come in many forms. If you're looking to prevent user accounts from becoming compromised, start with the easy—and often free—approach by implementing multi-factor authentication. For workstations, you'll want to ensure you have a Next Generation Anti-Virus installed to quickly identify potential ransomware from spreading while also remediating the attack. To protect your organization, you'll want to aggregate logs from devices on your network for continuous monitoring and incident response.

Andy Miller: As organizations adopt new technologies, information security will demand more time and attention. Essential antivirus and firewall systems are the first lines of defense, but traditional detection and response measures are inadequate. There are simply not enough personnel to provide manual security. Providers such as Pondurance provide a managed detection and response service that combines human and artificial intelligence to augment internal security systems. External vulnerability scanning tools, such as Acunetix, stress test a system's security protocols. At the account level, phishing reporting tools embedded within email services can minimize account attacks and stop further spread. Another helpful tool is TrendMicro, which offers Time-of-Click protection against malicious URLs in email messages, allowing the organization to block, filter, and mitigate email security risks.

Sponsored Content

Q: How should businesses respond to ransomware attacks?

Andy Miller: Ransomware attacks try to lure organizations to pay a "ransom" often in the form of cryptocurrencies, to reclaim organizational data held hostage with sealed encryption. The question is whether organizations should pay the ransom. Many cybersecurity analysts argue against this practice, noting that doing so empowers the bad actors and does not necessarily protect the data or organization. Wrestling with the payment issue will often devolve into a difficult decision that will depend on the firm and its operations. Being proactive by investing in business continuity practices, immutable backups, and infiltration prevention measures, is the only reasonable defense.

Ivan Shefrin: First, contact your local FBI field office. They have resources dedicated to helping solve cybercrime, even for small and medium sized businesses. Do not pay the ransom—there is a good chance you won't recover your data even if you pay. Not paying is a whole lot easier if you back up your critical data every day to an off-site location that supports what is called immutable storage (i.e., hackers can't encrypt or destroy your backup data). You'll need to contact a cybersecurity firm that specializes in digital forensics and incident response to help recover your data, understand how the bad guys got in, and recommend steps to make sure it does not happen again.

Stephen Daugherty: The first thing you should do if your organization is hit with ransomware is to isolate any machines that are affected. Once they have been removed from the network, you'll need to assess the impact. During the process, you'll need to determine how they got into your system, what accounts may be compromised and get your passwords changed. The next step is recovery; depending on the computer that was encrypted you'll need to decide whether you're going to restore from your backup or rebuild those machines.

Q: What advice do you have for businesses that are shopping for cybersecurity insurance?

Stephen Daugherty: The risk of cyber-attacks continues to grow, and industry experts anticipate further growth in 2023 as cybercriminals grow more sophisticated. This trend means massive changes in cybersecurity insurance programs across the industry. We have observed many new insurance renewal requirements, including multi-factor authentication and endpoint detection and response, to name a couple. When shopping for cybersecurity insurance, I advise seeking out an expert partner that can make sure you have the protection in place to maintain your coverage for today and for the future.

Andy Miller: Understanding the different categories and coverages needed when purchasing cyber insurance can help when pursuing a policy. The four categories of coverage include business interruption and extortion attacks, customer and employee data loss, payment fraud, and third-party liability (e.g., copyright infringement and unintended defamation). It is important to note that cybersecurity insurers consider your business liable for data breaches arising from third-party business partners. Organizations can be sued for their third party's inability to maintain adequate security controls.

Ivan Shefrin: Cybersecurity insurance underwriters are setting the bar higher, and premiums are going up for obvious reasons. If you have a security program in place already, with a plan to mitigate your highest risks first, you have a good chance of getting insurance at reasonable rates. But it's important to read the fine print. Make sure you understand what you're buying and understand what is or isn't covered by the policy. Consider using a broker who specializes in cyber insurance, as they can help explain the nuances.

Q: Staffing is a challenge these days. What are a few of the most valuable IT certifications a potential employee can have?

Ivan Shefrin: I personally value hands-on experience more than certifications, but it's certainly true that certifications help establish credibility—especially for people who don't have a lengthy resume of job experience.

In terms of IT overall, I always recommend that people start by learning networking since the Internet is so fundamental to business and the economy today. Cisco has several good certifications to get started. Also, for general IT operations, Information Technology Infrastructure Library Foundation is always a good place to get started.

For those interested in a career in cybersecurity, the Certified Information Systems Security Professional is a great certification because it covers such a wide range of information fundamental to the security practitioner. CompTIA Security is another good starting point.

Stephen Daugherty: If you're in the IT industry or you've been trying to build your business's IT team, you have probably noticed a shortage of talent in the field. The plus side of this for individuals is that it's a great time to grow your IT career. My perspective is to pick your niche and build up your certifications around that. As more and more companies continue to move to the cloud, certifications like AWS, Azure, and Salesforce are in high demand. As cybersecurity continues to be a concern, businesses will be looking to add cyber-specific roles to their team, so having Security+, CISSP, and CISA on your resume will certainly get you noticed. For an infrastructure focus, I suggest VMWare, Cisco, and Veeam certifications.

Andy Miller: The most in-demand roles in technology are programming, cloud computing, business applications, and information security. Training and certification in these fields provide entry- and mastery-level competency development. Programming training includes database management and an array of coding languages for various applications. Cloud computing involves the management of Amazon Web Services, Microsoft, Google, and Linux cloud infrastructures. Business applications include specific customer relationship management systems such as Salesforce and Hubspot, and enterprise resource planning systems such as NetSuite and Banner. A wide array of information security certifications provides a foundation and advanced knowledge in the field. Notable examples include CISM, CompTIA Security+, CISSP, and CISA, each with its unique level of sophistication. Access to this training is available from a variety of vendors and institutions. An example is Indiana Wesleyan University's Talent Ladder (thetalentladder.com), which provides training and a connection to a degree for those interested.

Q: What are a few IT positions that companies often lack that would serve them well as tech continues to advance?

Andy Miller: Advancements in technology will require more roles in security, cloud computing, business analysis, and project management. Growth in security and cloud computing is creating high demand for broadly accessible yet fortified technology. As noted earlier, the explosion of cybercrime will make security more important, yet consumers and businesses need the versatility of the cloud infrastructure. Balancing versatility and security will be an ongoing challenge for IT leaders and require qualified personnel. The demand for business analysts and project managers represents the increased complexity of IT work. Aligning organizational and end-user needs with the capabilities and capacity of the technology infrastructure will require roles in business analysis and project management. Business analysts translate the needs of end users into technical solutions while project managers ensure timely delivery of the solution. Both roles are vital to ensure the organization and its end users benefit from the technology infrastructure.

Ivan Shefrin: Ten years from now, many companies are going to have a chief data science officer and

See page 24A

Continued from page 23A

large teams working under that person. Machine learning already has a much greater role in our lives than many people realize. From the manufacturing floor to cars, marketing and robotics, machine learning is pervasive. One of many ML challenges is how to perform research and development without compromising the public's personal privacy. And what are the right policies and practices to ensure that developer's personal biases and perspectives do not impinge on the decisions and recommendations made by machine learning algorithms? In the rush to get new products and technologies out the door to gain competitive advantage, these decisions today are largely in the hands of technical developers without substantial organized guidance from leadership.

I believe most organizations will need to address this head-on, and the sooner we get started, the better. Data science does not only involve ethical decisions, which is the first thing people think of when we hear "personal bias" in training algorithms. It also addresses basic questions of business risk and liability.

Q: How can businesses partner with outside organizations to improve their technology ecosystem?

Stephen Daugherty: It's impossible for small businesses to maintain every internal IT role in-house without adding additional overhead. You need to identify the strategic partners that can work with you to achieve your goals for this year or the next 5 years. If you're not sure where to go, a strong partner can help you build that roadmap.

Ivan Shefrin: Given the complexity of information technology today, it's impossible for any organization—including the largest Fortune 500 firms—to go it alone without an ecosystem of trusted partners. Businesses can partner with managed service providers that can deploy and manage some or all their ecosystem. These resources can augment their existing IT staff. With the rise of cybercrime, networks now need 24/7 monitoring. Who is watching your network at 3 am on the weekends? One thing businesses must consider when partnering outside their organization is third-party risk. We have seen numerous cybercrime incidents occur because outside vendors and partners did not have the same level of cybersecurity controls in place as their customers, which creates back-doors for bad guys to steal their data.

Q: What other tech issues should be top-of-mind as businesses plan for 2023?

Ivan Shefrin: Artificial intelligence is continually improving, and it powers more applications and machines each day. Behavior-based technology is efficient, on duty 24/7 and less prone to error. IoT devices are becoming more and more widespread, they must be monitored, maintained, and secured. Cybersecurity and network architecture conversations must go hand in hand. Automation and digitization will make a lot of changes in customer experience when it comes to networks.

Economic uncertainty is top of mind for many business leaders today, and some may question the need to continue investing in cybersecurity. This is a mistake. Every business has a different risk profile, but customers and partners have higher expectations today than before. Companies are now starting to be held liable for poor cybersecurity practices, while good cybersecurity has become a competitive differentiator.

With security being a journey rather than a destination, I encourage readers to continue pushing forward with a cybersecurity program. The bad guys are not going to stop, and we need to continue being vigilant.

Stephen Daugherty: The last few decades have taught us that the standard corporate IT strategy is ineffective. Every organization must have a plan to address growing needs around cybersecurity. Hackers, malware, phishing assaults, and several other forms of cybercrime are wreaking havoc all over the world. This trend will only accelerate.

Andy Miller: In 2023, businesses will continue to experience rapid changes in cybersecurity and cloud computing. These areas will serve as cornerstones of the digital transformation that was afoot pre-pandemic but is now driving rapid changes in the economy. Firms of all sizes and types must respond to long-term consumer expectations that will change nearly every aspect of business. Artificial intelligence will become a competitive advantage for those that invest in this technology for sales, customer support, analytics, and operations. Augmenting current functions with AI will enable organizations to scale their work and provide consumers with more valuable products and services. Increasing demand for privacy in marketing and advertising will affect data collection and storage. Third-party data providers like Google will make it more difficult for organizations to identify prospective clients. On the individual level, the explosion of the Internet of Things will continue, increasing the complexity and opportunities for businesses.

SONDHI SOLUTIONS

Stephen Daugherty is Director of Technology for Sondhi Solutions, a technology staffing, strategy, and services firm. With over 20 years of information technology experience, Stephen leads the growth and acceleration of the lastest technology to Indiana companies.

INDIANA WESLEYAN UNIVERSITY

Andy Miller, PhD, serves as the vice president for innovation & partnerships at Indiana Wesleyan University. Andy establishes educational and strategic partnerships with various organizations in the Midwest, including workforce and economic development organizations, state agencies, corporations, local nonprofits, flight schools, and other educational institutions. These partnerships provide training and educational pathways to support adult learners and workforce needs.

COMCAST BUSINESS
Powering Possibilities™

Ivan Shefrin is the executive director of Managed Security Services for Comcast Business. He is a hands-on cybersecurity leader with 25-years of experience partnering with enterprise and communication service providers for security detection, threat intelligence, and incident response. He is responsible for Comcast Business DDoS mitigation, managed detection and response, and endpoint protection services.

Content paid for by Comcast Business, Indiana Wesleyan University and Sondhi Solutions.