Sponsored Content

THOUGHT LEADERSHIP SERIES

JULIE BIELAWSKI
Founder and CEO
Knowledge Services

BRODY ERTEL
Indiana Market Director
Meriplex

JOHN QUALLS
CEO and President
Purpose HQ and Eleven Fifty Academy, an Indiana Wesleyan Univerisity education pathway

CODY TYLER
Director of Infrastructure Operations
Sondhi Solutions

Cybersecurity & Technology

Cybersecurity requires constant vigilance

In our Thought Leadership Roundtable, experts at Indiana Wesleyan University's Eleven Fifty Academy, Knowledge Services, Meriplex, and Sondhi Solutions warn businesses not to take cybersecurity for granted and offer tips on how to secure your systems effectively.

Q: Cybersecurity is a rapidly evolving field. What, in your view, is the most pressing cybersecurity challenge organizations face today?

Julie Bielawski: One of the most pressing challenges from a business perspective is that cybersecurity is complex and perceived to be too costly to start. There is a need to de-mystify cybersecurity for businesses of all sizes, but especially for smaller organizations who are often uncertain where to start and who have more budget and bandwidth limitations.

On the technical side, two of the most pressing challenges evolving are how to manage third-party risks and how to address the role that Artificial Intelligence plays in cybersecurity. For example, a recent report by Adaptive Shield found that large companies rely, on average, on more than 4,000 cloud technologies. While the number for smaller organizations is less, the risk is still significant as cyber threats can come through any "cloud door." Without a thoughtful third-party risk management program, the risk severity is unknown.

Brody Ertel: One of the most pressing cybersecurity challenges organizations face today is advanced cyberattacks. Long-term, targeted attacks against organizations allow threat actors to remain undetected and exfiltrate valuable data over time. These attacks often combine multiple threat vectors like zero-day exploits, custom-made malware, and social engineering. Organizations must become adept in multiple areas of cybersecurity to counter these advanced threats. Ransomware is another challenge. Cybercriminals are now not only encrypting data but are stealing sensitive information before doing so. This dual threat increases the pressure on organizations to pay a hefty ransom to avoid data leaks.

John Qualls: In today's digital age, organizations across the board are confronting a common adversary: increasingly sophisticated cyber threats. These range from ransomware attacks, which can hold critical data hostage, to covert operations by nation-states and vulnerabilities lurking in supply chains. These heightened threats are further intensified by two major factors. Firstly, the IT environments are becoming more intricate, offering a broader surface for potential attacks. Secondly, there's a notable deficit in the number of skilled cybersecurity experts available to counter these threats. To stay ahead in this ever-evolving battlefront, it's not just about erecting firewalls or installing the latest antivirus software. The need of the hour is a comprehensive strategy that encompasses effective risk management, robust incident response mechanisms, and an emphasis on proactive sharing of threat intelligence. By weaving these into their cybersecurity fabric, organizations can fortify their defenses, ensuring the safety of sensitive data and the integrity of their infrastructure.

Cody Tyler: With the rapid adoption of diverse technologies, cloud services, Internet of Things devices, and remote work setups, organizations often struggle to gain a holistic view of their entire digital ecosystem. This complexity has made it challenging to identify vulnerabilities, unauthorized entry points, or potential weak links in their security chain.

To address this challenge, organizations need to invest in robust asset management, network monitoring, and cybersecurity auditing tools. Additionally, fostering a culture of cybersecurity awareness and promoting collaboration between IT and security teams are essential steps in gaining a better understanding of their digital footprint and mitigating associated risks.

Q: Cybersecurity requires being proactive. How can companies be proactive on the cybersecurity front?

Cody Tyler: First, start by assessing and identifying the specific risks your organization faces. Take a good look at your vulnerabilities and threats and prioritize them based on how they could impact your business. Next, put in place robust security measures tailored to your needs. This might include training your employees, keeping your software and systems up to date, enforcing strict access controls, and having a clear incident response plan. Lastly, remember that cybersecurity is an ongoing process. Regularly review and update your security measures to stay ahead of evolving threats, encourage a culture of cybersecurity awareness among your team, and keep a close eye on your network traffic and threat intelligence sources to detect and respond to new risks promptly.

Julie Bielawski: It is difficult to know where to begin, how to prioritize, or even where to turn next in your organization's ongoing cyber journey. If companies are not able or do not have the proper resources to achieve this, connecting with cyber experts or engaging with a cybersecurity advisor or consulting organization can help bridge the gap.

Sponsored Content

Brody Ertel: There are several measures companies can take to be proactive on the cybersecurity front. Organizations should conduct regular risk assessments to identify vulnerabilities, threats, and their potential impacts on the company. They should also establish comprehensive cybersecurity policies and procedures outlining security controls, acceptable use guidelines, incident response procedures, and more. Two other key areas that need strong technical controls are patch management and identity and access management. Ensuring that vulnerabilities are patched quickly and user identities are not compromised is critical to addressing cyberattacks. Lastly, companies must train their employees on cybersecurity best practices. The average employee now has access to several integrated apps and systems, making each individual staff member critical to successful cyber defense.

John Qualls: In the ever-evolving realm of cyber threats, companies must shift from a reactive stance to a proactive one. A crucial step involves routinely reviewing and updating security protocols, including conducting vulnerability assessments, and employing cutting-edge intrusion detection systems. The human element, however, cannot be sidelined. Continuous employee training, coupled with stringent access controls, is vital in mitigating risks. Furthermore, keeping abreast of emerging threats and adapting accordingly is essential to ensure a company's defenses remain robust and resilient against cyber adversaries.

Q: With the rise of hybrid work and cloud technologies, how can companies strike a balance between enabling seamless collaboration and maintaining robust data security?

John Qualls: By implementing a comprehensive cybersecurity strategy, companies can balance seamless collaboration and data security in hybrid work environments. This includes robust authentication protocols, encryption for data in transit and at rest, regular security training for employees, and continuous monitoring for potential threats. Employing cloud security solutions and collaboration tools with built-in security features can help ensure data protection while enabling effective remote collaboration and productivity.

Cody Tyler: Organizations should adopt a Zero Trust model, where trust is never assumed and multi-factor authentication is required for access. Data encryption, strong user access controls, and a principle of least privilege should be implemented. Additionally, selecting secure cloud service providers and conducting regular security training for employees are essential. Furthermore, endpoint security measures, data loss prevention tools, and collaboration platforms with strong security features should be in place. A well-defined incident response plan that covers remote and hybrid work scenarios is crucial, along with regular security audits and monitoring. Clear remote work policies, guidelines, and vendor security assessments should complement these efforts.

Julie Bielawski: This is a very real challenge faced by organizations today. Too often, perceptions prevail that to have robust data security, we must sacrifice business user experiences and collaboration. Both goals can be achieved, but it requires a philosophy that embraces education and commitment at the leadership level to ensure the right balance of robust data security policies are in place and integrated with an equally robust change-management process. Education and training are paramount in this effort, and each person should recognize his or her role in cybersecurity.

Brody Ertel: Striking a balance between enabling seamless collaboration and maintaining robust data security in a hybrid work environment and cloud technologies is crucial for organizations to get right. One way to achieve this is by implementing a Zero Trust architecture, which assumes no one inside or outside the network is trusted by default. This involves strict access controls for users and devices, regardless of location. Multi-factor authentication is another way to improve data security while allowing users access to necessary resources only. Robust endpoint security controls are critical to have in place as well. These include advanced anti-malware software, endpoint detection and response solutions, and remote device management software that enables rapid remediation of vulnerabilities, mobile device management, and strong encryption.

Q: Cyberattacks often exploit human behavior through social engineering tactics. How can education and training empower individuals to become the first line of defense against these tactics?

Brody Ertel: Education and training are critical in empowering individuals to become the first line of defense against social engineering tactics. Regular training sessions could teach staff to recognize social engineering tactics as well as phishing emails, links, and attachments using real-world examples. Lastly, employees should be trained in safe web-browsing habits, and learning to be cautious when clicking links, visiting suspicious sites, or downloading files from untrusted sources. Employees should learn to recognize the authenticity of emails, websites, and content in general.

John Qualls: Education and training are pivotal in empowering individuals as the first line of defense against cyberattacks. By educating people about common tactics like phishing, impersonation, and manipulation and providing practical training to recognize and respond to these threats, individuals can develop critical skills to safeguard sensitive information. Building a cybersecurity-conscious culture through ongoing education fosters vigilance, promotes responsible online behavior, and helps mitigate the impact of social engineering attacks, ultimately enhancing overall cyber resilience.

Cody Tyler: When you provide regular training to employees, you foster a culture of shared responsibility, where employees recognize their pivotal role in safeguarding data and assets. They won't just delete the email they think is suspicious but inform the cyber team of the attack, giving your organization more knowledge behind phishing scams. Comprehensive education and training not only equip individuals with the knowledge to combat social engineering tactics but also empower them with the confidence to do so effectively, thereby enhancing the organization's cybersecurity resilience.

Julie Bielawski: Embrace our motto: "See Something, Say Something." It's a straightforward yet immensely effective message for navigating the complex and dynamic threat landscape that has become a part of our daily lives. We believe that building cyber awareness among team members is as important to their personal lives as it is in the workplace. Our approach goes beyond the traditional methods, as we strive to integrate cyber education into our company's culture.

Education and training hold unparalleled significance as our first line of defense. Now, more than ever, the skill to communicate threats and risks with clarity and brevity has become the key differentiator between success and failure.

Q: Cybersecurity regulations and compliance standards are constantly evolving. How can organizations ensure they meet the latest requirements while maintaining a strong security posture?

Julie Bielawski: As supply chain risks grow, companies want and need to know that the technologies used can be trusted. Organizationally, adopting strategies known as Due Diligence and Due Care help operationalize a security program. Due Diligence centers on oversight, specifically how senior leadership directs resources to align with necessary strategic and

See page 32A

Sponsored Content

Continued from page 31A

regulatory compliance demands. Due Care focuses on actions. Establishing a Governance Risk & Compliance program serves as a cornerstone, enabling centralized management across an organization.

In our journey, we found that organizations can significantly benefit from implementing framework models such as StateRAMP, CorpRAMP, and Hi-Trust. These programs offer standardized risk management assessments and certification frameworks. They also streamline organizational priorities by providing clear guidelines and best practices.

Brody Ertel: Thankfully, many new regulations and compliance standards are based on security best practices. So, in many cases, compliance involves mapping existing security controls to new frameworks, rather than implementing new security controls. One effective method is to adopt a broad cybersecurity framework, such as NIST, ISO 27001, or CIS controls, as the baseline framework for your cybersecurity program. These frameworks typically form the basis for new requirements and regulations, making compliance easier.

John Qualls: Organizations should establish a robust compliance program to stay current with evolving cybersecurity regulations and compliance standards. This includes continuously monitoring regulatory changes, conducting regular risk assessments, and implementing adaptable security measures. Engaging in ongoing employee training and seeking external expertise can also help maintain a strong security posture and ensure compliance with the latest requirements. If that is outside their wheelhouse, ensure your service provider is accountable to these compliance standards.

Cody Tyler: Compliance is not a one-time thing; it is an ongoing effort. Continuously adapting and improving your security measures is paramount. This proactive approach ensures readiness to navigate and comply with any regulatory changes that may arise.

Make sure to appoint a dedicated compliance team to make sense of all these rules and ensure your organization follows them to the letter. Commit to regular risk assessments to spot any gaps between your current security setup and what the regulations demand, and then prioritize fixing them. Keep your policies and procedures up-to-date and train your team in what is expected.

Q: Cybersecurity can be intimidating, especially for smaller businesses. What advice would you give them?

Cody Tyler: Start small but remain consistent in your efforts to safeguard your assets and data as your business grows. First, tend to the basics: prioritize strong, unique passwords and enable multi-factor authentication for your accounts. Keeping software and systems up to date is crucial, as many attacks exploit outdated software. Second, identify your most critical assets and potential threats, and tailor your security efforts accordingly. Third, invest in employee-education training programs to make your employees the first line of defense.

If you lack an in-house team, consider outsourcing cybersecurity to a managed security service provider for cost-effective solutions that suit your needs. Implement regular data backups and test them to ensure you can recover from data loss due to cyberattacks. Don't forget network security, incident response planning, and compliance awareness. Engage with industry or local cybersecurity groups for support and consider cyber insurance to mitigate financial losses in the event of a breach.

Julie Bielawski: This is a question that is very personal to me, because it is our story. Our business has served the public sector for more than 25 years, relying on our cloud software that processes and stores confidential information. As we watched colleagues in the industry struck and devastated by cyber events, we knew we had to do more, but we did not know where to begin. We made missteps along the way that were costly, both in time and money.

That is why we have been so passionate about the development of RAMPxchange, a marketplace of ideas, experts, and a place for small businesses, like ours, to help guide them on their unique cybersecurity journey and avoid the missteps and false starts we experienced. My advice is to not go it alone, learn from others, and start today.

Brody Ertel: While it can be intimidating, cybersecurity is often just a matter of implementing a solid foundation and posture. Understanding the threats to your business, like data loss or service downtime, is the first step in establishing a robust cybersecurity program. Educating your teams, prioritizing your most critical assets, and implementing best practices, such as MFA, secure remote access, offsite data backups, and endpoint security come next. This would also be a good time to explore cybersecurity insurance options to mitigate the financial risks of a data breach or cyberattack. And lastly, consider seeking professional assistance from a reputable third-party organization. If you lack in-house expertise, consider working with cybersecurity consultants or managed security service providers to assess, implement, and maintain your cybersecurity defenses.

John Qualls: Smaller businesses should prioritize cybersecurity by enforcing complex password policies, keep software and systems up to date, installing reliable firewalls and antivirus software, regularly backing up critical data, conducting cybersecurity training, preparing a response plan for breaches, and considering outsourcing cybersecurity if resources are limited. You might be small but get the basics right!

Q: How does a Virtual Private Network enhance online privacy and security, and why should users consider using one?

John Qualls: A Virtual Private Network enhances online privacy and security by encrypting internet traffic, masking IP addresses, and providing anonymity. Users should consider using one to protect sensitive data, bypass geo-restrictions, and safeguard against cyber threats when browsing the web.

Cody Tyler: VPNs have become a crucial tool for ensuring a safer and more private online experience. Users should consider using VPNs, especially when using public Wi-Fi networks, to safeguard their data from potential threats. VPNs also provide an added layer of security for remote work or sensitive transactions.

Julie Bielawski: Cybersecurity is a journey, and VPN implementation can be one step along the way that encompasses education, organizational risk management, third-party risk management and more. For users seeking encrypted protection in an unencrypted public network, a VPN is a viable solution. However, it's crucial to understand that the VPN must be configured correctly to provide the highest level of security. Inaccurate setup can compromise the intended protection. It is also important to note that implementing a VPN does not constitute a robust security program. But it can be a step in providing a more secure connection.

Brody Ertel: All data traveling between a device and a VPN server is encrypted, making it extremely difficult for unauthorized third parties to intercept it. A VPN also protects the company by providing a secure tunnel for accessing corporate networks and resources, which also protects data from interception. This allows the company to keep those resources within their internal networks instead of accessible over the Internet, thus preventing attacks directly on those resources.

Q: How crucial is collaboration between public and private sectors to tackle cybersecurity challenges effectively?

Brody Ertel: Collaboration between the public and private sectors is critical for effectively addressing cybersecurity challenges. Public sector organizations like government agencies and law enforcement often have access to classified or sensitive threat data, giving them a broader view of the cyber threat landscape. This can help private

organizations prepare for advanced cyber threats. Also, many critical infrastructure sectors like energy and transportation are privately owned but essential for everyday life. Public-private collaboration is crucial to protect these critical assets from attacks. Another point to consider is that the government is ultimately the source of the regulations and standards businesses must adhere to. Collaboration with the private sector can ensure these regulations are practical, effective, and not overly burdensome.

John Qualls: Collaboration between the public and private sectors is crucial to tackling cybersecurity challenges. Public entities can provide regulatory frameworks, threat intelligence sharing, and law enforcement support, while private companies offer technical expertise, innovation, and critical infrastructure protection. Ultimately, this synergy is essential to safeguarding digital infrastructure and maintaining the security and trust of individuals, businesses, and governments in the digital age.

Cody Tyler: Both sectors bring unique strengths to the table. Government agencies can provide valuable threat intelligence, regulatory frameworks, and legal support while private companies contribute expertise, innovation, and resources.

Julie Bielawski: We are fighting an invisible war. Cyberattacks and threats are ongoing, and the only way to combat the challenges is to work together. The success of businesses and the protection of our way of life demand collaboration. It is an area where the government has led, and industry is catching up.

While there have been notable strides over the past three years, there is still much to be done. That is why it has been our mission to create a place that brings together both the public and private sectors in this invisible war we are fighting and what led us to create RAMPxchange.

Q: What emerging trends do you believe will have the most significant impact on cybersecurity in the next five years?

Cody Tyler: The integration of artificial intelligence into cybersecurity will likely lead to significant changes in how organizations protect their digital assets. AI promises and already is revolutionizing threat detection by analyzing massive datasets in real-time, identifying anomalies, and recognizing previously unknown threats more effectively. This will enable faster incident response and proactive defense measures.

However, alongside these benefits, there are challenges to consider. Cybercriminals may also employ AI to create more sophisticated malware and craft convincing phishing attacks, posing a constant challenge for defenders. Organizations will increasingly rely on AI-powered security analytics to make sense of the overwhelming volume of security data, prioritize alerts, and conduct threat hunting.

Julie Bielawski: The duality of AI and Machine Learning, along with quantum computing, are key trends to watch. Platforms like ChatGPT and similar large language models are freely accessible to the public, fostering a generation growing up alongside these tools that will surely enhance them.

Additionally, an ongoing issue is limited cybersecurity talent, which is a problem that will continue to grow. This strategic threat requires comprehensive action to overcome and will only be achieved through collaboration between industry and community.

Brody Ertel: AI and machine learning-powered attacks have the greatest potential impact on cybersecurity, and we are already seeing it. Threat actors can use large language models like ChatGPT to generate more effective phishing and social engineering attacks. Conversely, cybersecurity professionals are leveraging AI and machine learning to identify and respond to threats more effectively. The ongoing arms race between AI-powered attacks and defenses will shape the cybersecurity landscape.

Another significant impact will likely come from the commoditization of attacks for monetary gain, such as ransomware. This backing will make it easier for cybercriminals to launch attacks, posing a significant threat to organizations and lowering the barriers to entry for threat actors.

John Qualls: In the next five years, emerging trends like quantum computing, AI-driven attacks, and IoT growth are set to have a substantial impact on cybersecurity. Quantum computers may break current encryption methods, while AI will enhance both defensive and offensive capabilities. The rapid growth of IoT devices presents a broader attack surface. Additionally, supply chain vulnerabilities and increased remote work will demand robust cybersecurity measures to protect against evolving threats. If I had to pick one, it would be AI-driven attacks. The social engineering that AI can mimic will be a significant challenge.

knowledge services

Julie Bielawski is founder and CEO of Knowledge Services. Her guiding principle, "Serving Those Who Serve Others," captures her dedication to making a meaningful impact. Her commitment to providing best in class services, technologies and security leaves a lasting mark, embodying leadership, empathy, and an unwavering commitment to a safer digital future.

MERIPLEX

Brody Ertel founded Cyberian Technologies in 2005 to provide owners, leaders and IT managers with creative technology solutions to improve their businesses. In 2021, Cyberian Technologies was acquired by Meriplex and Ertel stayed on as Indiana Market Director, helping businesses leverage IT for a competitive advantage and ensure their business is protected from cybersecurity threats.

Eleven Fifty Academy

John Qualls, CEO and President of Purpose HQ and Eleven Fifty Academy, an Indiana Wesleyan University education pathway, has a three-decade record of success in the technology industry. With a deep understanding of the technological trends and cycles that have shaped today's hosted IT environments, he has successfully implemented a range of innovative solutions that have elevated his organizations to new heights of success.

SONDHI SOLUTIONS

Cody Tyler serves as Director of Infrastructure Operations at Sondhi Solutions. He is an accomplished strategic IT and cybersecurity leader. With more than 12 years of experience in diverse industries, he is recognized for his value-driven approach, creating and guiding high-achieving teams, introducing data-centric risk management frameworks, and adeptly conveying intricate cybersecurity ideas to non-technical audiences.

Content paid for by Indiana Wesleyan University, Knowledge Services, Meriplex, and Sondhi Solutions.