Sponsored Content

THOUGHT LEADERSHIP PANEL
IBJ MEDIA CONTENT STUDIO

JORDAN JOHNSON
Cybersecurity Senior Consultant
Dean Dorton

CODY TYLER
Managing Director
EXOS CYBER

CHRIS YOUNG
Director of Cybersecurity Services
GadellNet Consulting Services

Cybersecurity & Technology

Cybersecurity requires savvy, vigilance

In this week's Thought Leadership roundtable, experts from Dean Dorton, EXOS CYBER, and GadellNet Consulting Services advise businesses on the best practices for keeping their information safe and recovering from cyberattacks when breaches happen.

Q: What are examples of emerging cybersecurity threats and how can companies stay ahead of the curve as threats evolve?

Jordan Johnson: One of the biggest emerging threats revolves around business email compromise attacks. Business email compromises are when business emails are compromised and then used to attack other businesses. There are publicly available toolkits, such as Evilginx, that allow threat actors to easily spin up phishing kits to target organizations. These solutions can also be used to bypass multi-factor authentication and pose a big risk for organizations large or small. The biggest thing organizations can do is stay informed. Read articles regarding the latest trends and how to defend against them.

Cody Tyler: Emerging cybersecurity threats, such as advanced ransomware and sophisticated phishing attacks, are growing more dangerous as attackers use new tools and techniques. To combat these, companies need to focus on robust defenses like regular data backups, strong access controls, and continuous monitoring for unusual activity.

To stay ahead of evolving threats, businesses should invest in threat intelligence, regularly update their security practices, and conduct frequent security assessments. Leveraging automated security tools and adopting a proactive security mindset can help detect and respond to threats quickly. Ongoing employee training and well-prepared incident response plans are also crucial for enhancing overall security and ensuring a swift recovery from potential attacks.

Chris Young: One of the most common threats we've seen in late 2023 and 2024 are brute force attacks, particularly against a VPN. In this scenario, a threat actor attempts to log into a corporate VPN with a predetermined list of usernames and passwords to see if they can get into the environment. Once inside, the threat actor can move undetected, gather reconnaissance, steal proprietary information, and potentially infect the entire organization with ransomware.

To stay ahead of the curve, organizations should invest in technology that allows fast, agile protection if faced with a cybersecurity incident. We have partnered with Blackpoint Cyber to use our toolsets to help increase our speed of detection and alert for our clients. This allows us to get ahead of the situation, begin remediation, and analyze what happened. Together, this reduces downtime and the overall impact of an incident.

Q: How can businesses leverage Artificial Intelligence to better protect themselves from cybersecurity threats?

Cody Tyler: Businesses can use AI-driven tools to detect and respond to threats faster than traditional methods. AI can analyze vast amounts of data in real-time, identifying patterns and anomalies that indicate potential attacks, such as phishing or malware. Machine learning algorithms can predict new threats by learning from past incidents, enabling proactive defense measures. AI also automates repetitive security tasks, freeing up human resources for more complex problem-solving. By continuously adapting to new threats, AI helps businesses strengthen their security posture, reduce response times, and minimize the impact of cyberattacks.

Chris Young: AI is designed to automate tasks and eliminate busy work so individuals can prioritize higher-payoff activities. AI is becoming one of the big buzzwords in technology, and more tools are utilizing AI to analyze malicious threats, parse information, and take action on your behalf.

AI itself can also exacerbate threats. Organizations should exercise caution when entering information into AI tools like ChatGPT. Most AI tools will keep a log of what you enter. This data can be viewed by a threat actor, exposing your organization to risks unseen through traditional security tools. AI is a great tool that can be leveraged for a variety of purposes. Just remember a threat actor can also leverage these tools. It is essential to begin thinking about security tags and protocols for your organization's data, allowing you to restrict or designate access for company-approved AI tools.

Jordan Johnson: AI can make a cybersecurity professional's job easier by allowing them to automate certain tasks. It should be seen as an assistant that can be used to make decisions based on the data you feed it. At the very least, it can be used to make initial decisions until a human can take a look.

Q: Give us examples of how security solutions can be customized to meet the unique needs of specific clients.

Chris Young: This can happen in several ways. The most common way is to use exclusions in each security solution. An exclusion tells software that this is a known file or program that is acceptable to run in the environment. We often see situations where anti-virus solutions cause issues in mission-critical applications.

The other important way to customize your security solution is by parsing

information down to the level most important to you. Security solutions supply copious amounts of data to parse and generate alerts. These alerts can generate even for expected activity and can cause what's known as alert fatigue if not parsed effectively. Taking the security solution and disabling alerts that you do not care about can reduce the amount of noise generated and parse the information down to only the activity that is not authorized.

Jordan Johnson: Most security solutions offer robust customization options. A good example of this is endpoint detection and response tools. They allow operators to set up workflows to perform certain actions, like automatically isolating a host if high risk is detected. Security is never a cookie-cutter, one-size- fits-all solution. It must be tailored according to various factors like industry, size, etc.

Cody Tyler: Security solutions can be customized by tailoring defenses to industry-specific needs, such as enhanced encryption and compliance management for health care (e.g., HIPAA) or advanced fraud detection in financial services. Small businesses may require simplified, cost-effective security measures like managed detection and response (MDR) services, while larger enterprises need scalable solutions with AI-driven threat hunting and incident response automation. Customization also includes adjusting access controls, deploying specific monitoring tools, and aligning security policies to match the client's risk profile, regulatory requirements, and operational environment, ensuring tailored protection that addresses unique vulnerabilities.

Q: When a security breach occurs, how quickly should a business expect a response from its tech provider, and what should that response look like?

Jordan Johnson: Ideally, an organization would want their IT provider to respond within minutes. Cyberattacks are no longer a slow-build process. They are often smash-and-grab, meaning a lot of damage is done rather quickly. The response should revolve around initially containing the incident and ensuring the threat- actor is evicted. Then restoration and recovery efforts can commence.

Cody Tyler: Following a security breach, a business should expect a response from its tech provider within an hour. The response should include immediate containment actions, such as isolating affected systems and blocking further unauthorized access. The provider should quickly investigate the breach's cause, assess the impact, and begin remediation efforts. Communication is key: the provider should offer regular updates, guidance on next steps, and support in notifying affected parties if needed. A detailed incident report should follow, outlining the breach, corrective actions taken, and recommendations to prevent future incidents.

Chris Young: This is an interesting question because the response portion depends on the type of incident. From a response perspective, the tech provider should, at minimum, call to alert you to an investigation. Our team will gather some initial information while investigating so that we can provide details during that initial call. Our goal is to avoid the "what happened?", "I don't know" awkward conversation that can sometimes occur initially. You should expect this level of quality to be better from your service provider.

It gets more complicated when you talk about what the response should look like. If an email account gets hacked and it's managed by the tech provider, the response is going to be quick. However, if it's something like your company's Facebook account, that will involve reaching out to Facebook to help remediate. Your tech provider should be able to guide you on how to resolve the issue.

Q: How can businesses build back stronger after a cyber security attack?

Cody Tyler: Organizations should conduct a thorough post-incident analysis to identify vulnerabilities and implement corrective measures. Strengthening security includes updating software, enhancing firewalls, and tightening access controls. Investing in advanced threat-detection tools and employee training, and regularly updating incident response plans is essential. Businesses should also review and refine their data backup and recovery strategies to minimize future downtime. Engaging in regular security assessments and staying updated on emerging threats ensures that the organization remains resilient and better protected against future attacks.

Chris Young: The best action is to put security at the forefront. Often, organizations that fall victim to a cybersecurity attack are organizations that have not developed policies, do not provide training, or have allowed antiquated technology to remain active in their environment.

Some essential security measures, like implementing dual control (requires two people to send a payment out of the organization) or separation of duties immensely reduces the risk of your accounting department falling victim to a phishing email.

Another area is honestly just knowing what you already have in your environment. Microsoft 365 and Google have a lot of security tools built into their licensing, like conditional access rules, built-in spam filtering, and even alerts. You can save thousands of dollars on the latest and greatest tool by simply knowing what's currently available to you and adjusting administrative processes accordingly. After those foundational pieces, you can invest more effectively in your cybersecurity stack.

Jordan Johnson: The goal is to make progress so that an attack does not happen again. This includes following recommendations from the IT provider or incident response firm that was engaged during the incident. Businesses should structure their security using a defense-in-depth posture, where there are no single points of failure. The longer it takes an adversary to complete their actions, the more likely it is that they give up or are caught by security analysts.

Q: Do small businesses need cybersecurity-specific insurance or is an umbrella policy enough? What are the key components of a robust policy?

Chris Young: Small businesses need cybersecurity-specific insurance. Umbrella policies tend not to include verbiage for cyber issues, or they contain a flat amount of coverage for all incidents, both in the cyber and physical world. A cybersecurity-specific policy will take the controls already implemented in your organization and take your revenue into consideration to create a policy that is tailored to your needs as a business.

Jordan Johnson: This primarily depends on the business. If a business has a limited online presence and does not process any sensitive or financial information, it might make more sense from a budgetary perspective to go with an umbrella policy. If that is not the case, cyber-specific insurance is recommended. Key components of a robust policy are: providing financial relief, forensic capabilities and legal counsel in the event of a cyberattack.

Cody Tyler: Small businesses typically need cybersecurity-specific insurance rather than relying solely on an umbrella policy. Cybersecurity insurance covers data breaches, ransomware, and other digital threats, offering critical support for incident response, legal fees, and customer notification. Key components of a robust policy include coverage for data breach costs, business interruption losses, legal liabilities, and extortion payments. It also should provide access to expert services for breach response and recovery.

Q: What criteria should businesses use when selecting technology vendors or partners?

Jordan Johnson: Google is honestly your best friend here. Research the company. See if they have

See page 24A

Sponsored Content

Continued from page 23A

had any cyber incidents and, if so, what happened. Ask them probing questions about how they will ensure your company is not put at risk. See if they are SOC2 compliant or compliant with other compliance models. Do your due diligence.

Cody Tyler: To ensure a good fit, it's important to first assess the vendor's security practices, including their adherence to industry standards and regulatory compliance to protect your data. Examine their reputation and reliability by checking customer reviews, industry ratings, and their track record of delivering services. The vendor's solutions should be scalable, allowing for growth and adaptation to your evolving needs. Consider the quality and availability of customer support and service to ensure timely assistance. Compare pricing with the value offered, ensuring the solution fits your budget and provides a strong return on investment. Finally, verify that the vendor's technology integrates smoothly with your existing systems to avoid compatibility issues.

Chris Young: Outside of costs, terms of the agreement, options, etc., I think the biggest criteria should be a demonstrated understanding of your current and future business goals. A technology partner should be able to identify your specific needs and respond in a way that helps you grow and scale. They should feel like an extension of your organization and not the vendor attempting to make a sale. A good partner will understand your needs and bring solutions to the table to help you adjust as technology advances. If an organization doesn't feel valued, there will be a lack of trust if something goes wrong (like a cybersecurity incident). Having a strong partnership and trust in your service provider allows you to grow faster and, when an issue occurs, be confident you're being taken care of as effectively as possible.

Q: How can businesses plan for scalability when implementing new technology solutions, ensuring they can grow without significant disruptions?

Cody Tyler: To plan for scalability, businesses should select flexible, cloud-based technology that can adjust with growth. Design systems with modular components that allow for easy upgrades. Assess how solutions handle increased demand and integrate automation to streamline processes. Choose vendors with robust support and scalable infrastructure. Regularly review performance and scalability needs and adjust as necessary to align with business growth. This approach helps ensure technology can expand smoothly, minimizing disruptions and supporting long-term success.

Chris Young: Plan for scalability by developing a plan and being methodical in deployment. Having the right partner—internal or outsourced—to assist in this undertaking ensures technology is deployed with limited interruptions. When deploying a solution, like a new security tool, it's important to start with a pilot group and deploy to a limited number of individuals before deploying globally.

Once the solution is in place, it's important to create automation to make sure the software is installed as new devices come onto the network, whether it is through growing the organization or simply replacing old devices with new ones.

Jordan Johnson: The biggest factor is planning for where you're wanting to go, not where you are now. It's easy to get tunnel vision and be laser-focused on one area. Infrastructure is a concern. Cloud-based options such as Entra or Amazon Web Services can help make this easier. It's flexible and you can deploy or decommission when you need it. In summary, look at placing infrastructure in the cloud.

Q: What are the best practices for managing the human side of technological change, including employee training and adoption?

Chris Young: You need to understand your personnel and know what training is needed. While every organization wants to be secure, understanding your audience helps dictate what controls should be implemented. Individuals have varying job functions and not all training is necessary for all job responsibilities. Understanding your environment, your team, and their responsibilities will allow you to develop customized training for everyone. The results will save you time and money.

Jordan Johnson: Including end users in change discussions can help this process. Organizations with mature security and technology programs often implement steering committees that allow employees from various departments an opportunity to give their input. This helps with managing technological change.

Cody Tyler: To manage technological change, clearly communicate benefits, provide thorough training, involve employees early, and offer ongoing support. Address concerns promptly and ensure resources are available to help with the transition. This fosters acceptance and smooth adoption of new technology. We should also remind our users that they are not the problem but give positive feedback when correct actions are taken.

Jordan Johnson is Cybersecurity Senior Consultant for Dean Dorton. He has more than five years of information technology experience, in roles ranging from IT support technician and systems engineer to systems administrator. He currently works on the defensive side of security, ensuring that client networks meet best practices and are hardened against ever-evolving cyber threats.

Cody Tyler serves as Managing Director of EXOS CYBER. He is an accomplished strategic cybersecurity and IT leader. With more than 14 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.

Chris Young is GadellNet Consulting Services' Director of Cybersecurity Services. Young began working in IT in 2008 as an engineer while continuing earning a master's degree from Michigan State University in Cybercrime and Digital Forensics. He is a trusted consultant for GadellNet clients, always striving to deliver exceptional security and results.

Content paid for by Dean Dorton, EXOS CYBER, and GadellNet Consulting Services.