LOS ANGELES BUSINESS JOURNAL

CYBERSECURITY + DATA PROTECTION

TECHTALK SERIES

WEDNESDAY, OCT. 30

Sheraton Universal Hotel

8:30AM-11:00AM PST

To register, visit labusinessjournal.com/events/techtalk2024

DIAMOND SPONSORS

AON

COMCAST BUSINESS

PLATINUM SPONSORS

IMA

MARYMAN
INCIDENT RESPONSE · INVESTIGATIONS · DIGITAL FORENSICS

Nth GENERATION

WGU
THE UNIVERSITY OF YOU

LOS ANGELES BUSINESS JOURNAL
CYBERSECURITY + DATA PROTECTION
TECHTALK SERIES

In today's digital age, businesses face an array of threats to their cybersecurity and data integrity. From sophisticated hackers to internal vulnerabilities, the need for robust strategies to protect sensitive information has never been greater.

Join the Los Angeles Business Journal on Wednesday, October 30 for a comprehensive breakfast discussion dedicated to exploring the latest advancements, best practices and emerging trends in business cybersecurity and data protection. Our expert speakers and panelists will dive into key topics, providing invaluable insights and practical guidance to help businesses safeguard their digital assets and maintain trust with customers, partners, and stakeholders. **Don't miss this opportunity to stay ahead of the curve to protect your business in an increasingly digital world.**

AGENDA

8:30AM	Breakfast & Networking
9:00AM	Welcome Remarks
9:15AM	Keynote Speaker
9:35AM	Cybersecurity + Data Protection Technology Solutions
10:20AM	Risk Management & Prevention Strategies
11:00AM	Closing Remarks & Networking

To register, visit labusinessjournal.com/events/techtalk2024

THE PANELISTS

KEYNOTE SPEAKER

Founder of the US Navy Cyber Counterintelligence Program at Naval Criminal Investigative Service (NCIS) and former chief of cybercrime intelligence at the Microsoft Cybercrime Center will be giving a 15-minute talk about cyber breaches. Having directed cyber espionage and cyber terrorism operations for decades, and then helping some of the world's most preeminent companies through ransomware and other attacks, Bryan will be covering the cyber threat landscape, what you should do *before* a breach and the in the room reality of the first 12 hours and next 30 days *after* a breach.

BRYAN HURD
Managing Director, Aon Cyber Solutions
Aon

CYBERSECURITY + DATA PROTECTION TECHNOLOGY SOLUTIONS

MIKE GRANT MODERATOR
Principal, National Cyber Risk Practice
Marsh McLennan Agency

TERRANCE COOLEY
Cybersecurity Instructor, Fullstack Academy
Western Governors University

JEROMIE JACKSON
Director, Security & Analytics
Nth Generation

KEVIN McADAM
Chief Revenue Officer
One Step Secure IT

KIMBERLY PEASE
Vice President / COO
Maryman

RISK MANAGEMENT AND PREVENTION STRATEGIES

JON KORIEL MODERATOR
Manager, Public Affairs
Comcast

PETER K. JACKSON
Counsel
Greenberg Glusker

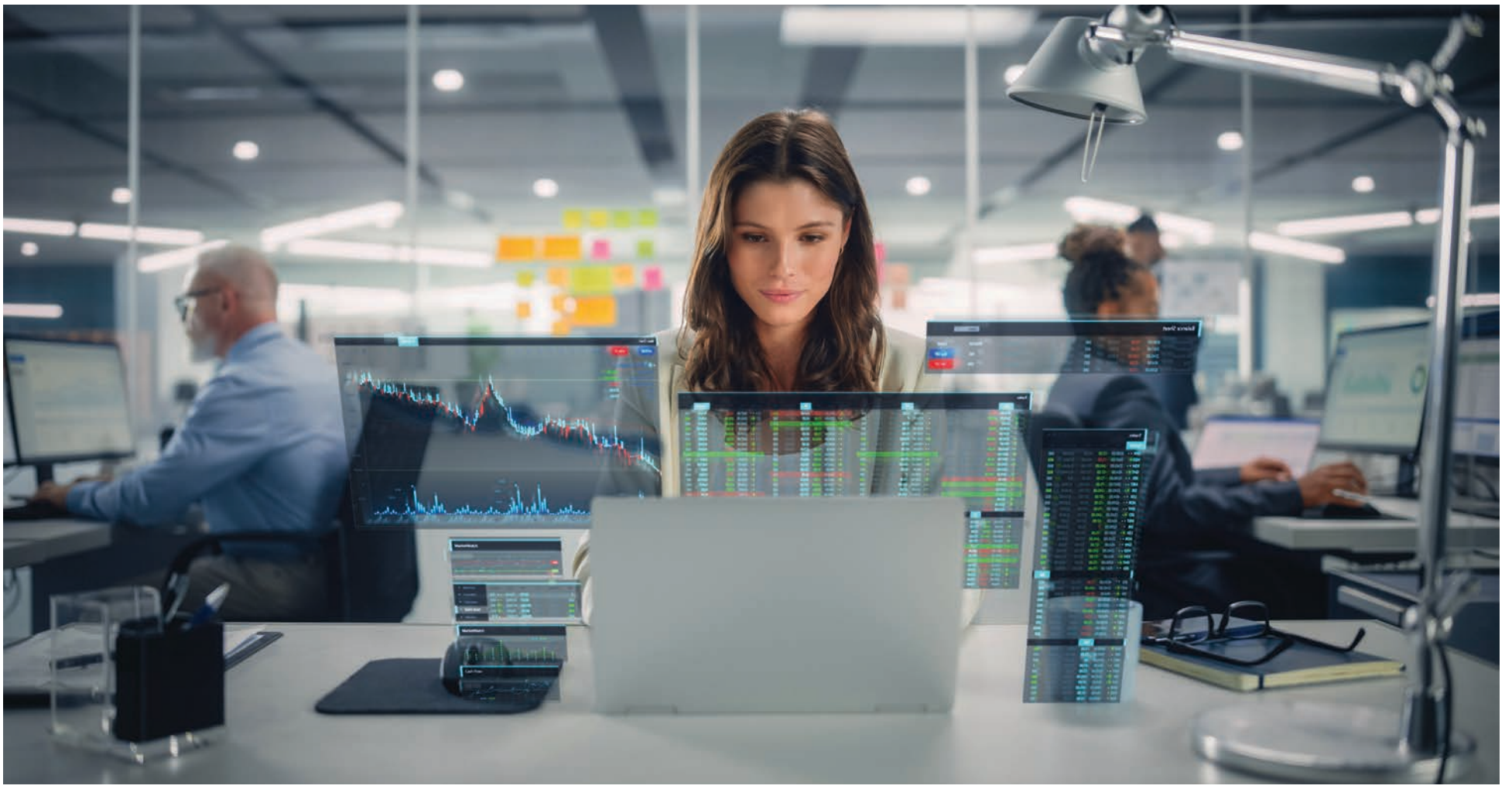
CRAIG MYERS
Vice President
IMA Financial Group, Inc.

IAN SCHWARTZ
Managing Director; West Region Leader, Cyber Solutions
Aon

JASON THOMPSON
Security Specialist
Comcast

Comcast Business now powers businesses in Los Angeles with reliable connectivity and secure networking solutions that help mitigate cyberthreats. Learn how enterprise managed services from Comcast Business can help you create better customer experiences. Powering global enterprises. Powering Possibilities.™

LOS ANGELES BUSINESS JOURNAL
CYBERSECURITY + DATA PROTECTION
TECHTALK SERIES



Protecting Any Organization from Cyber-Attacks

By WILLIAM BOECK and CRAIG MYERS

Search for "major cyber-attacks in 2024" on Google, and you'll be met with an astounding list that barely scratches the surface of the issue, showcasing only a fraction of the reported incidents.

While the good news is that many attacks are thwarted by robust cyber defenses before any harm can be done, the bad news is equally concerning. Cyber-attacks have doubled between 2016 and 2022, and data breaches surged by 73% since 2021. In fact, the average payout for these breaches reached a staggering $1.54 million in 2023.

Ransomware attacks are the number one cyber threat facing organizations in the United States, and phishing remains the most widely used attack vector among cyber criminals. These attacks, sent in emails, texts, or by phone, are intended to trick victims into sharing sensitive information or giving criminals control over their computer systems. If successful, criminals can access sensitive data or deploy malware that locks users out of technology, forcing organizations to pay a ransom.

What cyber criminals want most is a payday. Just a few years ago, most went 'whaling,' targeting multinational corporations looking for monster payouts. Today, cyber criminals prefer to 'trawl' for victims, understanding that smaller organizations and businesses are vulnerable because they lack budgets to build out a robust protective cyber shield.

MANAGING CYBER RISK

As ransomware and other cyber risks are growing, it is essential for organizations to understand and actively manage their unique risks. Every organization needs to have basic risk controls in place. Cyber insurers now require this before they insure an organization.

When considering what to include in a cyber risk program, consider a strategy that focuses on three areas:

- Implementing protection that hampers or avoids attacks.
- Implementing protocols to detect breaches and attacks.
- Building resilient, offline backup infrastructure.

Multi-factor authentication (MFA) is a great starting point. It requires one extra step when signing in beyond a password, creating an effective deterrent. MFA is included in out-of-the-box SaaS applications such as Microsoft 365 and Google Suite.

Email protection is another layer of security that detects and prevents threats such as spam and spoofed emails, a basis of phishing attacks. Like MFA, email protection is part of many SaaS applications.

A third, essential measure is a back-up strategy. Backing up data to a secure, offline destination isolated from the main network and regularly testing those back-ups can ensure a quick recovery from a cyber event.

Patching software with appropriate frequency and avoiding software that its creator no longer supports are critical elements of cybersecurity. Tens of thousands of software vulnerabilities are discovered every year. Software companies quickly release fixes for critical vulnerabilities, but it is up to users to apply these fixes, known as "patches." Over time, developers stop supporting old versions of their software. Vulnerabilities in such software will not be fixed, making the use of end-of-life software very risky.

Endpoint detection and response (EDR) is another important cybersecurity measure. EDR products bring threat detection and response to individual computers and network hardware to prevent computer viruses and malware from entering the computer system.

Finally, cybersecurity training for employees is absolutely essential. Employees need to be able to spot phishing emails, take steps to avoid social engineering fraud, and safeguard the organization's data and IT environment.

These are just a few of the security measures organizations can implement, and there are many others that offer even greater protection. Most companies may not be able to adopt every control immediately, and that's fine. By starting with the basics, organizations can establish a strong and affordable defense that delivers essential protection.

CYBER RISK MANAGEMENT DOES NOT ELIMINATE CYBER RISK

Good cybersecurity measures will minimize cyber risks, but they can't eliminate them or their financial consequences. That's where cyber insurance comes in. Cyber risk management and cyber insurance combine to build a defense to protect organizations from cyber events and a financial backstop with respect to the losses – including business downtime and reputational harm, that such an event can cause.

Cyber policies should be adaptable to address the specific risks that an organization prioritizes. Since each insurer's cyber policy is unique, it is possible to tailor the coverage to meet those specific needs.

Ransomware attacks are the number one cyber threat facing organizations in the United States, and phishing remains the most widely used attack vector among cyber criminals.

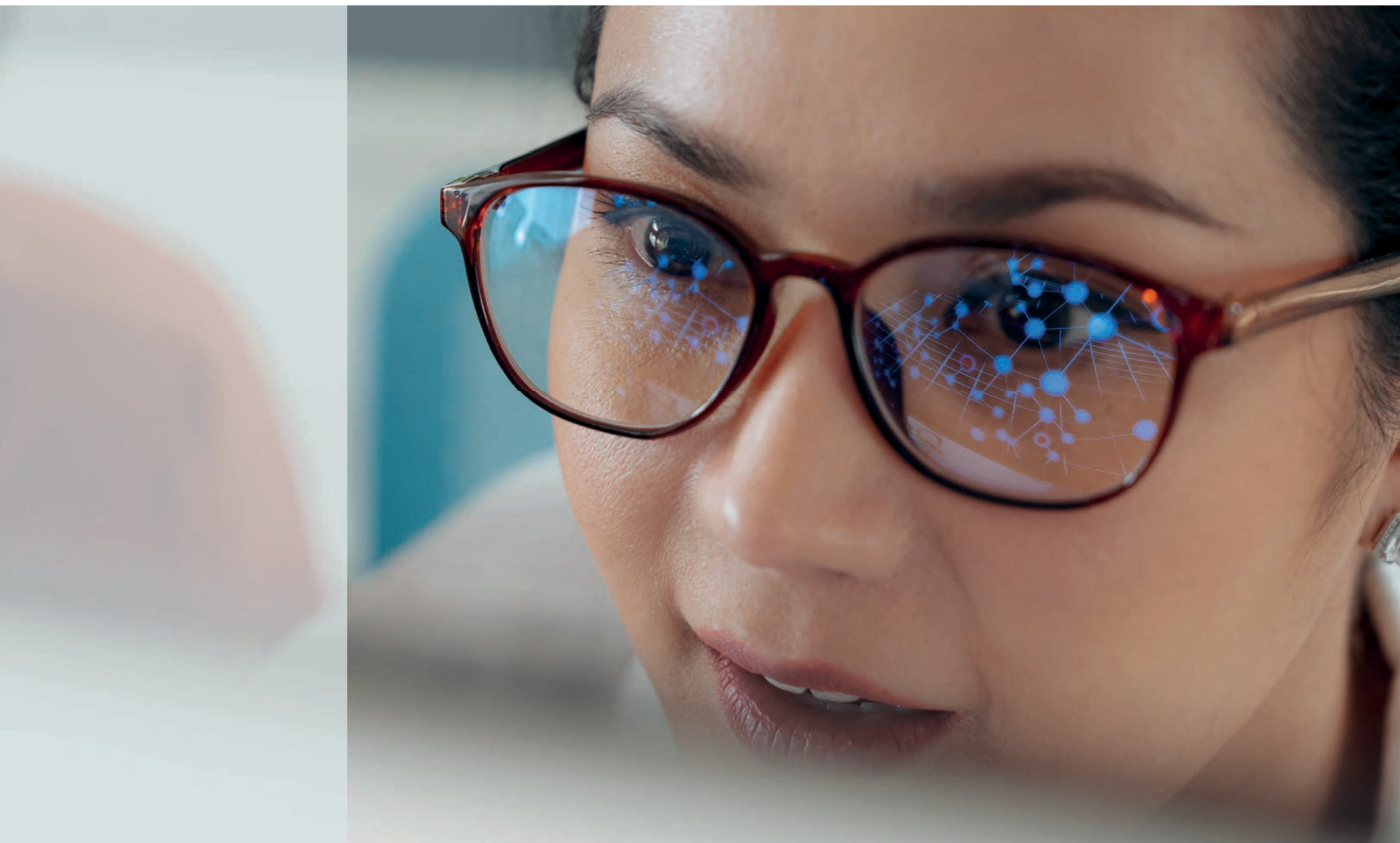
Cyber policies offer benefits beyond just covering losses. Many insurers also provide free or discounted loss control services that assist companies in implementing essential cybersecurity measures. Since the types of services vary by insurer, it's crucial to consider these offerings when choosing a cyber insurance provider.

William Boeck is executive vice president, cyber product leader, for IMA Financial Group. Craig Myers is vice president, commercial lines, for IMA Financial Group. Learn more at imacorp.com.

Aon is in the Business of Better Decisions

As a trusted advisor, Aon helps clients around the world manage cyber risk and build sustained cyber resilience. Regardless of industry, size or geography, we give our clients the clarity and confidence to make better decisions to protect and grow their businesses.

www.aon.com/cyber-resilience



LOS ANGELES BUSINESS JOURNAL
CYBERSECURITY + DATA PROTECTION
TECHTALK SERIES

Artificial Intelligence Drives New Era of Cyber Threats and Defenses

Report analyzes 29 billion attempted cybersecurity attacks against Comcast Business customers

Comcast Business recently released its 2024 Cybersecurity Threat Report, a valuable resource for IT and security professionals, based on the analysis of 29 billion cybersecurity events detected by Comcast Business across its security customers in 2023. The report highlights significant changes in the cybersecurity landscape, driven by sophisticated threat actors, an expanding attack surface and the transformative power of AI.

"Armed with a newfound arsenal of AI-based capabilities and a landscape littered with vulnerable systems, cybercriminals are having a moment," said Noopur Davis, chief information security and product privacy officer with Comcast Corporation. "Our findings confirm that despite these advancements, a multi-layered approach combining advanced protection, detection, managed services, and vigilant maintenance of security practices, can help enterprises protect their digital assets and enhance their resilience against sophisticated threats."

This report offers a comprehensive overview of the rapidly evolving global cyber threat landscape, based on cybersecurity events detected by Comcast Business across its security customers in 2023. The report highlights an intensifying global threat landscape, including the following:

• AI amplifies cyber risks but offers powerful tools to mitigate threats.

For both bad actors seeking to steal corporate data and IT security professionals tasked with protecting it, AI is changing the rules of engagement. Defenders are increasingly utilizing AI and machine learning to analyze malware and log data at scale, as well as to scan entire systems for anomalies and automatically respond to threats. AI can act as a force multiplier for defensive teams working to safeguard their organizations and data.

• Phishing attacks are on the rise, threatening businesses worldwide.

Phishing remains the primary method used by attackers to gain initial access to networks, with over 2.6 billion interactions detected by Comcast Business. Additionally, over 90% of the phishing interactions Comcast Business blocked were designed to direct victims to phishing sites hosting malware. The trend underscores the need for robust anti-phishing technologies, user education, and email gateway platforms to combat this growing threat.

• Bad actors are employing advanced lateral movement techniques to navigate networks.

Remote services were the most exploited method for lateral movement, with over 409 million events detected by Comcast Business. Employing tools like Endpoint Detection and Response (EDR) and Managed Detection and Response (MDR) can help IT staff identify early-stage threats by monitoring network activity for anomalies in user behavior. They help protect devices connected to enterprise networks by using AI to proactively detect, investigate, remove, and remediate malware, phishing, and ransomware.

• Attackers are increasingly using encrypted channels and proxies to hide their command and control (C&C) communications.

By exploiting these protocols, attackers can mask their malicious activities and evade detection. Domain Name System (DNS) tunneling remains a popular technique to bypass traditional security measures, with over eight million observed events. Similarly, Transmission Control Protocol (TCP) was used in 104,000 events to provide reliable communication channels, often with encrypted payloads that further obscure malicious activities. The use of Windows Remote Management (WinRM), which saw nearly 78 million events, was also prevalent. These methods underscore the need for sophisticated detection tools to identify and mitigate covert malicious activities.

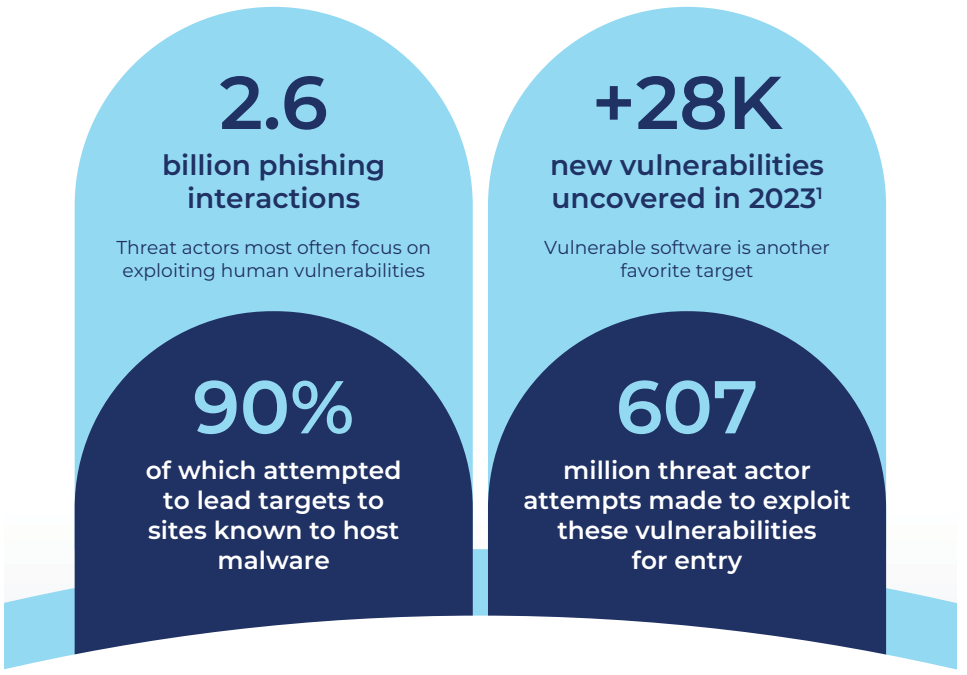
> 'Our findings confirm that a multi-layered approach combining advanced protection, detection, managed services, and vigilant maintenance of security practices, can help enterprises protect their digital assets and enhance their resilience against sophisticated threats.'

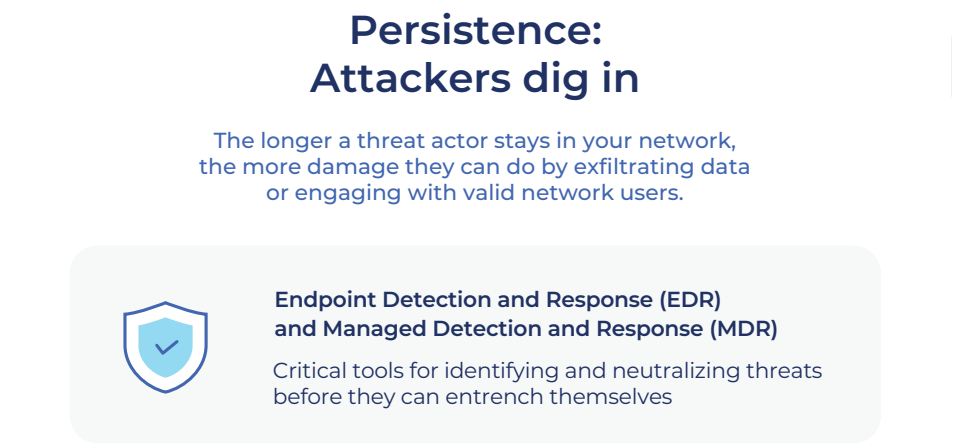
• Distributed Denial of Service (DDoS) attacks and ransomware pose significant risks.

Comcast Business identified and blocked over one billion attempts to destroy data. Additionally, there were more than 126 million blocked instances of malware or botnets designed specifically for financial theft, underscoring the financial motivations behind many cyber-attacks. DDoS attacks remained a major threat to Comcast Business customers, with 103,000 reported events. This surge emphasizes the need for robust DDoS protection and mitigation strategies.

The report provides CISOs, CIOs, and security leaders with a deep dive into how cyber threats can breach and then spread across global networks. This analysis enables them to make informed security decisions for protecting critical assets. The report's trends and findings underscore the importance of adopting a multi-layered approach to cybersecurity to bolster defenses against evolving global threats.

To learn more about Comcast Business's advanced cybersecurity solutions, or to access the full 2024 Comcast Business Cybersecurity Threat Report please visit business.comcast.com/enterprise/products-services/cybersecurity-services.





EARN A RESPECTED DEGREE ON YOUR TERMS

WGU's School of Technology offers programs that fit your budget and busy schedule. Whether you're interested in cybersecurity, cloud, IT, software engineering, computer science, data analytics, or another related field, earning a WGU degree is your first step to a cutting-edge career in tech.

Bradley B., B.S. IT—Network Operations and Security

COMPETENCY-BASED EDUCATION

WGU offers a wide variety of bachelor's, master's, and certificate programs across the business, technology, education, healthcare, and nursing fields.

Each program is developed with input from industry experts specifically for our unique online-learning platform. Progress is measured by proficiency. You can even rely on your existing knowledge to move through courses more quickly.

LOW, FLAT-RATE TUITION

Tuition varies by program and is charged per six-month term. Terms begin the first of any month. You can take as many courses as you are able each term at no additional cost.

Undergraduate program tuition starts at $3,725 per term.

Graduate tuition starts at $4,040 per term.

All required program materials are covered by a flat $200 resource fee paid each term. Visit wgu.edu to view all available programs and their accompanying costs.

IN A 2023 HARRIS POLL SURVEY OF 300 EMPLOYERS OF WGU GRADS...

98%

SAID GRADUATES MET OR EXCEEDED EXPECTATIONS

97%

SAID THEY WOULD HIRE ANOTHER WGU GRADUATE

WGU

Learn more
wgu.edu/technology
866.225.5948

LOS ANGELES BUSINESS JOURNAL
CYBERSECURITY + DATA PROTECTION
TECHTALK SERIES

A Middle Market Roadmap for Cyber Resilience

Middle market organizations face unique challenges in the ever-changing cyber environment, requiring holistic insurance solutions and enhanced resilience readiness to manage risks that could impact profitability.

KEY TAKEAWAYS

- Some middle market firms may not purchase cyber insurance coverage or invest in cyber security to the extent required to defend against evolving cyber risks.
- While middle market cyber insurance purchasing trends are shifting, further education on available risk transfer solutions and a well-rounded cyber readiness plan are necessary.
- Brokering partners in the cyber risk landscape can help middle market organizations navigate the insurance marketplace to find competitive solutions.

Cyber attacks and data breaches continue to rank as the top global threat companies face today – a threat exemplified by events like the global CrowdStrike outage, which put companies' incident response plans to the test and demonstrated that even non-malicious cyber incidents may have serious repercussions.

Middle market organizations are particularly exposed in this evolving risk environment due to historical underinsurance trends and cyber readiness plans.

FOUR MYTHS IMPACTING THE MIDDLE MARKET'S CYBER PREPAREDNESS

Midsize organizations face a unique set of challenges that heighten cyber risks. As a company grows, so too does the importance of understanding these risks to ensure a clear path to cyber resilience. However, there are many existing myths to watch out for that can interfere with a firm's cyber readiness journey:

Myth #1: Middle market firms are not targeted by bad actors to the same extent as large organizations.

Cyber events can have an impact on all areas of an organization. They are industry – and size – agnostic. Regulatory bodies are also tightening cyber security requirements, which could impact middle market firms' exposures to risk if unprepared to abide by the rules. Moreover, middle market companies often handle significant amounts of valuable data, including personal customer information, financial records, and intellectual property, making them a prime target for bad actors.

Myth #2: Midsize firms don't need to invest in cyber security.

This trend is changing as middle market companies focus more heavily on cyber security. Nonetheless, bad actors are looking for low-hanging fruit, irrespective of size. If a midsize client leaves the door open, they're going to extract what they can from that organization. "Technology and cyber risks have evolved far more rapidly than middle market companies' ability to both handle their exposures and purchase insurance to transfer cyber risks," explains Brent Reith, Aon's head of Cyber Solutions in North America.

Myth #3: Cyber policies are unaffordable and difficult to obtain for non-buyers.

While the hard market a few years ago may have made this true for some companies, the current soft cyber insurance market is competitive for first-time buyers who might still be in the process of implementing safety controls.

"The rising tide of cyber security maturity globally is lending itself to a more buyer-friendly market," says David Molony, head of Cyber Solutions for EMEA. "In addition, the cyber insurance market is opening itself to become much more available to first-time buyers."

Myth #4: Cyber Coverage is included in other policies that middle market firms purchase.

Midsize organizations may mistakenly believe that they have cyber coverage as part of their other insurance policies. However, traditional commercial insurance policies might not be designed to explicitly address cyber-related losses. If a policy does not affirmatively grant or exclude cyber coverage, this is termed "silent cyber," and there's no guarantee that it will cover a loss.

By purchasing standalone cyber insurance coverage, middle market organizations can counteract the risk of insufficient cover in the face of increasing cyber threats.

THE CYBER RISKS FACING THE MIDDLE MARKET

Seventy percent of all organizations report they are prepared to navigate new exposures, but just 36 percent say the have adequate application security measures in place. In the middle market specifically, organizations typically retain more risk. Many still don't purchase cyber insurance coverage and, if they do, they don't purchase it to the level of coverage or limits they need.

HOW MIDDLE MARKET ORGANIZATIONS CAN ACHIEVE CYBER RESILIENCE

The pressure is on middle market firms to not only continuously block and tackle bad actors, patch vulnerable systems, and understand the connection points across highly integrated technology stacks, but also stay on top of the potential impact of emerging threats and regulatory changes.

176%

Ransomware attacks spiked 176 percent in the first half of 2023, while the price tag of a single enterprise data breach rose to a historic high of nearly $4.5 million.

Source: Aon's Global Risk Management Survey

As a result, security and technology teams in the middle market must constantly evaluate their preparedness for evolving threats and provide quantifiable evidence of current controls effectiveness to insurers and the marketplace.

Midsize companies can build sustained cyber resilience by managing the full cyber life cycle through the four points of assess, mitigate, transfer, and recover:

- **Assess:** Understand the organization's security posture and its current level of cyber resilience. Use analytics to benchmark cyber security resilience against peers in the market and identify weak points to make better decisions on risk management and cyber insurance solutions.
- **Mitigate:** Be proactive to help minimize the impact of cyber threats, using tools that can help defend against active threats, while also planning for incident response and rehearsing that response with attack simulations.
- **Transfer:** Turn to risk transfer solutions and work with a partner that can provide access to improved insurability, pricing, and scope of coverage. Organizations can better navigate the insurance-buying process by identifying control deficiencies and prioritizing improvements prior to approaching insurance carriers, to minimize Q&A and be viewed as a more appealing risk to insurers.
- **Recover:** When a cyber attack occurs, middle market firms need to have processes in place to respond effectively in real-time. Research the causes of the incident and take concrete steps to become more resilient against future attacks.

To execute a cyber resilience strategy successfully, organizations should focus on access to risk transfer solutions backed by competitive pricing and broad coverage terms, strong client claims advocacy, proactive cyber security consulting, effective response incident planning and analytics-backed loss scenario modeling.

In light of the evolving cyber risk landscape, middle market organizations should strive to partner with a broker that has a pulse on how cyber risks are evolving – one that brings (re)insurance expertise and can anticipate shifts in the retail cyber insurance market before incidents occur.

Learn more at aon.com/cyber-resilience.

AI is here to stay. What are you doing to adapt securely?

ASK YOURSELF

AI: Could leveraging open-source LLMs be the most practical & fastest way to leverage AI for your organization?

What's best for your organization: ChatGPT or a private intelligent chatbot? And when is one or the other a better approach?

When is the last time you did a Ransomware Readiness test?

Has your IT environment been tested with an AI-powered penetration test yet?

What are your organization's external risk and susceptibility to ransomware scores – based on your IT vendors, supply chain, and the information currently available in the dark web and other open source intelligence?

Explore how Nth Generation can help you kick start your AI projects:

Start with some of the use cases most rapidly being adopted:

- Build your private intelligent chatbot – deploy vetted open-source LLMs while protecting your most valuable data and AI-generated insights
- Boost your security posture via AI-powered computer vision - deploy your own private, scalable modern video surveillance

Discover how Nth Generation can help you improve your overall security posture against increasingly sophisticated AI-powered cyber attacks while containing skyrocketing costs.

Nth is here to help.

Scan QR code to schedule a 1 on 1 with a Subject Matter Expert to further discuss these topics...

Nth GENERATION | Nth Security

Nth Generation provides comprehensive IT Security, leveraging industry leading services & technologies. Utilize our security brain trust -- comprised of an awarded, tenured CISO team. Our cybersecurity professionals possess an average of 21 years of experience. These experts assist in identifying vulnerabilities and provide remediation recommendations. www.nth.com

LOS ANGELES BUSINESS JOURNAL
CYBERSECURITY + DATA PROTECTION
TECHTALK SERIES

Artificial Intelligence, Security Risks, and Ransomware Readiness: Navigating the Future of Cybersecurity

By JEROMIE JACKSON

Artificial intelligence (AI) is revolutionizing industries, including cybersecurity, where it helps automate tasks and enhance threat detection. However, AI also creates new attack vectors that adversaries are eager to exploit. Understanding these risks, staying ahead of evolving trends, and preparing for ransomware attacks through technical readiness assessments are critical for modern organizations.

This article explores AI-driven security risks, current cybersecurity trends, and the importance of ransomware readiness assessments to ensure organizations are equipped to defend against sophisticated threats.

AI-DRIVEN SECURITY RISKS: NEW ATTACK VECTORS

AI is a powerful tool for both attackers and defenders. While it strengthens security systems, it also introduces vulnerabilities that can be exploited. The MITRE Atlas framework highlights how attackers use AI to automate malicious activity and target AI systems themselves.

One significant threat is model poisoning, where an attacker corrupts the training data that AI models rely on, causing the system to make inaccurate decisions. For instance, attackers can manipulate AI models to allow malicious traffic or evade detection.

AI also enables automated phishing and social engineering attacks. By using AI, attackers can craft highly personalized messages, making phishing attempts more convincing and harder to detect. Additionally, AI-generated malware can continuously evolve, bypassing traditional security systems.

However, AI can also be a defense tool. It improves anomaly detection, threat hunting, and incident response, automating routine security tasks and providing rapid insights into suspicious activities. But as organizations adopt AI-driven tools, they must remain vigilant about securing their AI models and data from manipulation.

KEY CYBERSECURITY TRENDS: STAYING AHEAD

Several trends are shaping the future of cybersecurity, and staying informed is vital to protecting against AI-enhanced threats.

1. AI-Augmented Security: AI is now essential in security operations, helping to detect threats, monitor behavior, and respond to incidents. However, as AI adoption grows, so do the risks. Organizations must protect their AI systems from adversaries who might manipulate models or data.

2. Zero Trust Architectures: The rise of remote work and cloud environments has eliminated traditional network perimeters. Zero trust models, which continuously verify every user and device, have become critical in securing distributed networks.

3. Cloud-Native Security: As businesses migrate to the cloud, traditional security solutions are insufficient. Security tools designed for cloud environments, such as container security and micro-segmentation, are necessary to protect cloud-based infrastructure.

4. Ransomware Resilience: Ransomware remains one of the most significant threats, and defending against it requires more than reactive measures. Proactively testing an organization's ability to withstand a ransomware attack is essential to resilience.

5. Automation and Orchestration: The complexity of modern cyber threats demands faster, more efficient responses. Security automation helps accelerate incident response, while orchestration streamlines workflows, reducing the burden on security teams.

These trends highlight the importance of adopting proactive strategies that incorporate AI, zero trust models, and cloud-native security tools to stay ahead of both traditional and AI-enhanced threats.

RANSOMWARE READINESS: EVALUATING DEFENSE CAPABILITIES

Ransomware attacks are a constant threat, and their frequency is only increasing. Organizations must regularly assess their technical capabilities to respond to ransomware attacks effectively. A Ransomware Readiness Assessment (RRA) evaluates how well an organization's defenses can detect, mitigate, and respond to a simulated ransomware attack. Unlike broader program assessments, RRAs focus on technical resilience, ensuring organizations can withstand real-world ransomware tactics.

KEY COMPONENTS OF A RANSOMWARE READINESS ASSESSMENT

1. Simulated Ransomware Attack: The RRA begins with a controlled simulation of a ransomware attack, mimicking real-world tactics used by attackers, such as data encryption attempts and command-and-control (C2) communication. This allows organizations to observe how their systems react in real time.

2. Defense Evaluation: During the assessment, the organization's detection and response capabilities are analyzed, identifying potential gaps in security infrastructure. This includes evaluating the performance of tools like firewalls, intrusion detection systems (IDS), and endpoint detection and response (EDR) solutions.

3. Risk Identification: The RRA identifies specific vulnerabilities that could be exploited during a ransomware attack, such as misconfigured systems or unpatched software. A detailed report outlines these vulnerabilities and provides actionable recommendations for improving the organization's defensive posture.

4. Mapping to MITRE ATT&CK: The techniques used during the simulated attack are often mapped to the MITRE ATT&CK framework, which helps organizations understand the tactics used by ransomware attackers. This structured approach enables targeted improvements in specific areas of defense.

CONTINUOUS TESTING FOR LONG-TERM RESILIENCE

Ransomware readiness is not a one-time activity. As ransomware evolves, organizations need to conduct regular technical tests to ensure their defenses remain up to date. Continuous testing allows security teams to adapt their strategies as new attack techniques emerge, ensuring long-term resilience.

By identifying and addressing vulnerabilities early through technical readiness assessments, organizations can build robust defenses and improve their ability to respond to ransomware attacks. Regular assessments also provide valuable insights that inform broader security strategies, ensuring organizations are prepared to handle a wide range of threats.

CONCLUSION

As AI continues to reshape cybersecurity, it brings both opportunities and risks. Organizations must leverage AI to enhance their defenses while remaining aware of the new attack vectors it creates. At the same time, ransomware remains a formidable threat, requiring organizations to take proactive steps in testing their defenses.

Technical ransomware readiness assessments provide critical insights into an organization's ability to defend against ransomware. By simulating attacks and identifying vulnerabilities, organizations can strengthen their defenses and stay resilient in the face of an ever-changing threat landscape.

Combining AI-driven security tools with regular readiness assessments and continuous testing is essential for building long-term resilience against both AI-driven threats and traditional ransomware attacks. Organizations that stay proactive and informed will be better positioned to navigate the complex and evolving cybersecurity landscape.

Jeromie Jackson is director of security & analytics at Nth Generation. Since 1991, Nth Generation has provided award-winning consultative IT services, encompassing a suite of IT and security solutions. Nth boasts top technical and consulting talent and expertise – as well as numerous industry leading manufacturer partnerships – spanning IT infrastructure and advanced cyber security technologies, frameworks, and services. For more information, questions, or assistance in establishing best practices, contact Nth Generation at (800) 548-1883 or visit Security.Nth.com.

To connect with an Nth Subject Matter Expert on Nth's solutions & services, visit nth.com/nth-survey.

DEFENDING YOUR DATA, PROTECTING YOUR BUSINESS

In today's fast-paced, digital world, businesses face growing risks from cyber threats and data breaches.

Maryman has been a leader in digital forensics and cybersecurity with **more than 100 combined years of experience, delivering expert solutions to protect organizations and navigate complex legal challenges.**

- **Computer Forensics**
- **Incident Response**
- **Investigations**
- **eDiscovery**

MARYMAN®
INCIDENT RESPONSE · INVESTIGATIONS · DIGITAL FORENSICS

SECURE YOUR BUSINESS TODAY!

For more information or to schedule a consultation, visit **www.maryman.com** or e-mail us at **joe.greenfield@maryman.com**.

Call: **818-290-3775**

LOS ANGELES BUSINESS JOURNAL
CYBERSECURITY + DATA PROTECTION
TECHTALK SERIES

Top Five Myths of AI and Cybersecurity

By PAUL BING and RICHARD BENBOW

The global rise of increasingly sophisticated cybercrimes creates daily challenges for the cybersecurity industry as security professionals grapple with new and evolving attacks, complex IT architecture, and the integration of artificial intelligence (AI) into nefarious actors' tactics, techniques, and procedures (TTPs). As a result, cybersecurity practitioners feel a sense of urgency to stay at the forefront of technological advances to defend against a growing arsenal of exploits. In this environment, a methodical approach to the intentional use of AI for cybersecurity protocols will help avoid falling prey to the hype and myths of groupthink such as these five myths of AI and cybersecurity:

1. You'll fall behind if AI isn't your primary solution for cybersecurity.

While AI can enhance cybersecurity tasks by analyzing large volumes of data to identify nefarious, it can also be susceptible to false positives and negatives, be trained on bad data, or act in unexpected ways. Many common cyber threats can still be effectively mitigated through basic security practices like strong passwords, regular patching, and employee awareness about social engineering. Incorporating AI into security solutions is not a license to abandon proven tools and replace established best practices. Sophisticated attackers will find ways to evade AI-based detection, so adopting AI cannot be the only solution for security and defense. Time-tested security practices like organizational culture, leadership commitment, and employee training are still critical fundamentals of a robust organizational risk management practice.

2. Threat actors are using AI, which will lead to an exponential increase in cyberattacks.

AI is undoubtedly a powerful tool that can be used for both good and bad, it's not a guaranteed game-changer for threat actors. The cybersecurity landscape is a dynamic battleground, and the interplay between AI-powered attacks and defenses is complex. AI may increase the speed and sophistication of certain attacks, such as better phishing attempts; however, it has not fundamentally changed the attack vectors or the attack surface within organizations. A mature security posture using foundational defensive practices continues to be a sound approach to reducing risk and thwarting attacks.

3. AI-powered tools are better, and every tool needs an AI feature.

AI-aided tools can provide powerful additions to a defensive infrastructure with quicker, more comprehensive data discovery. Left unchecked, AI is capable of producing sometimes comical but altogether bad results such as the Google Overview suggestion of adding glue to homemade pizza sauce or the McDonald's AI drive-through putting bacon on ice cream. In cybersecurity, erroneous results have serious consequences including loss of trust, excessive costs, and endangering human safety. The potential benefit of any AI-powered resource must be balanced against the potential cost of error. The safest use of AI is within a layered defense model which allows for verification and redundancy in protetive solutions.

4. You can only combat AI with AI.

AI is a valuable tool in the cybersecurity quiver, but it's not impenetrable. Like any other defensive technique, attackers can exploit vulnerabilities in AI models or develop exploits to bypass AI defenses. Combating AI threats requires a multi-layered approach that combines AI with human expertise, traditional security measures, and a strong focus on prevention, detection, and response. Using AI to combat AI may also raise ethical and legal concerns, particularly around issues like autonomous decision-making, accountability, and potential for misuse. These concerns must be carefully considered before implementation to ensure responsible, ethical use of AI in cybersecurity. By leveraging the strengths of both humans and AI, organizations can build a more resilient and effective cybersecurity posture.

5. AI is going to replace your job.

Companies hiring fewer entry-level people into cybersecurity roles are not doing so because AI has eliminated those jobs; instead, they are limited by shrinking budgets and a need to hire people who can make an immediate impact when they come on board. AI excels at automating repetitive tasks, analyzing vast amounts of data, and identifying patterns. However, human intuition and judgment are still needed to interpret those insights, make critical decisions, and adapt strategies to combat evolving threats. At its best, AI allows humans to focus on creative and strategic thinking to deliver complex problem-solving. The prominence of AI has created new jobs, such as AI engineers and AI ethicists, to manage AI systems. AI-related roles and cybersecurity roles will continue to emerge and evolve. AI won't replace people, but people who know how to work with AI may replace people who don't.

Effective cybersecurity requires a multi-layered approach that combines technology, processes, and people. Solely relying on AI for cybersecurity can create a false sense of security, and AI-based cybersecurity solutions can be costly and complex. While AI is transforming the workforce, it's unlikely to lead to widespread job displacement. Instead, it will likely change the nature of work and require adaptation and development of new skills. Progressive companies will see the value of investing in training programs and implementing policies that support workforce transition. Organizations looking to maximize their security posture with enhanced value, productivity, creativity, and innovation will find AI a valuable complement to existing people, systems, and processes.

Paul Bingham is the senior vice president and executive dean at Western Governors University's School of Technology, which currently serves 58,000 students nationwide and is the top conferred of cybersecurity degree in the country. Prior to WGU, Bingham spent 24 years as an FBI agent, leading and managing domestic and international cybersecurity investigations and FBI SWAT teams on over 100 high-risk tactical missions.

Richard Benbow is the regional vice president (West) of Western Governors University, where he leads efforts to provide affordable, high-quality education to underserved adult learners. He combines his expertise in innovation and IT with a commitment to student success, driving value for students and employers. Benbow holds an MBA from the University of Michigan, an MA in Emerging Communication Technology Policy from USC, and a BS in Business Management from Howard University. His prior roles include leadership positions at UCLA and Time Warner Cable.

It’s not a matter of **if** a cyber breach will happen to your company, it’s a matter of **when.**

IMA’s vigilant team of experts can help you get **cyber insurance** in place before it’s too late.

Craig Myers
Vice President
craig.myers@imacorp.com
661.964.7469

LOS ANGELES BUSINESS JOURNAL
CYBERSECURITY + DATA PROTECTION
TECHTALK SERIES

Technology Shouldn't Be Your Only Cybersecurity Defense

By KIMBERLY PEASE

In the late 1990s, as the chief information officer (CIO) for a 24/7 manufacturing firm, one of the owners asked me, "Are we secure?" With the utmost confidence, I replied, "Yes. We have industry-standard antivirus software, a secured enterprise firewall, perimeter locks, and backup tapes that I personally take offsite weekly." I had provided a solid, technically sound answer, and we both moved on, convinced we were effectively safeguarding the organization's sensitive information and network infrastructure.

Now, as a seasoned expert in Information Security—commonly known as cybersecurity— looking back with a "cybersecurity lens," I can't help but cringe.

MANAGING CYBERSECURITY: BEYOND IT

All too often when speaking with business professionals, I still hear them confidently assert, "My IT department is handling security."

Cybersecurity is not merely an IT issue; it's a vital function that demands a risk-based approach rather than just an IT-centric solution. Organizations must adopt comprehensive strategies that extend beyond traditional IT measures.

Most organizations proactively manage financial, regulatory, legal, operational, competitive, and reputational risks. Yet, when it comes to cyber risk, many still lack formal management or frameworks and continue to look only for technical solutions.

CYBERSECURITY REPORTS AND EXECUTIVE MANAGEMENT

Many typical departments within business provide management with regular detailed reports—financial, sales, performance, productivity and more. However, IT departments often neglect to deliver relevant reports on cybersecurity, leaving a significant gap in managing enterprise risk.

IT should be encouraged to provide management with cybersecurity reports such as vulnerability and patch management reports, IT security assessment key findings, significant incident summaries, documented remediation efforts including lessons learned.

Even though IT and executive management speak two different languages, reports, graphs and summaries can be universal in bridging the gap.

POLICIES AND STANDARDS: THE FOUNDATION OF CYBERSECURITY

Information Security policies and standards are essential—they are the foundation of any cybersecurity management program. Standards like ISO/IEC 27001 and NIST's Cybersecurity Framework provide guidelines that facilitate businesses and IT in meeting legal standards and commercial reasonableness when complying with appropriate best practices and contractual and regulatory requirements.

Regular security audits and assessments are vital for identifying risks and the most common critical vulnerabilities. However, policies and standards alone are not enough. Businesses must foster a culture where everyone is invested in security.

SOPHISTICATED ATTACKS VS EDUCATED EMPLOYEES

Employees are the key to a security-aware culture. Employees can unknowingly expose the company to cyber threats by clicking on malicious links or using weak passwords, often without the knowledge of executive management. A security-first culture empowers employees to make safer choices.

Organizations can cultivate a security-first mindset, where everyone is protecting the organization's digital assets. In today's fast-paced environment, where technology enhances efficiency, it is entirely possible to maintain a security-aware culture that supports speed and security simultaneously.

INCIDENT RESPONSE: PREPARE WITH THE RIGHT TEAM

Despite the best preventive measures, cyber incidents will occur. A tested incident response plan, guided by stakeholders, is vital for minimizing damage and ensuring cyber resilience. The plan should include key team members from legal, HR, IT, and forensics. Regular drills are essential to prepare the response team for swift action that aligns with stakeholder expectations.

A common pitfall is that IT professionals, in their urgency to restore systems, may compromise digital evidence. Including legal and forensics experts on the team beforehand is critical to preserving evidence and securing attorney-client privilege, which can mitigate the risk of lawsuits.

CONCLUSION: A HOLISTIC APPROACH TO CYBERSECURITY

Managing cybersecurity requires a comprehensive approach that goes beyond IT. Organizations should be implementing robust policies and standards, promoting security-conscious behavior, ensuring effective IT governance, and weaving cybersecurity into their overall business strategy. It's essential to recognize that cybersecurity is not merely a technical issue; it's a critical business imperative that requires the commitment of the entire organization.

Instead of asking your IT manager, "Are we secure?" business should strive to answer, "Our organization manages the protection of sensitive information and network infrastructure through a formal program that includes appropriate policies, ongoing training, and a culture of security awareness from the top down. We continuously assess and adapt our IT measures to address emerging threats in maintaining our cybersecurity posture."

Kimberly Pease is vice president and chief operations officer of Maryman. Learn more at Maryman.com.

Experts Stress Need for Businesses to Improve Cybersecurity Effectiveness

The recent "Audit Committee Practices Report: Common Threads Across Audit Committees," a joint effort between Deloitte's Center for Board Effectiveness and the Center for Audit Quality (CAQ), identified cybersecurity as their top priority moving forward.

A total of 266 respondents participated in this year's survey, most of whom are from US public companies (74%), and of which 81% have more than $700 million in market cap.

Respondents cited enterprise risk management (ERM) as the No. 2 priority, demonstrating a broader, more holistic view of risk. Meanwhile, trending topics like artificial intelligence (AI) governance and environmental, social and governance (ESG) reporting are receiving comparably less attention.

"We are seeing the role of the audit committee continue to evolve and adapt as demands on oversight responsibilities change with the business environment and investor expectations," said Vanessa Teitelbaum, senior director, Professional Practice at CAQ. "Audit committees are zeroed in on one of their core responsibilities: overseeing enterprise risk programs at large. While their agenda continues to grow and expand, key areas like cybersecurity and ERM remain a central focus."

In addition to cybersecurity and ERM, finance and internal audit talent (a new entry in this year's survey), compliance with laws and regulations, and finance transformation rounded out the top five priorities. Although the majority of respondents view internal audit as an effective function — one that adds demonstrable value — nearly 80% believe there is an opportunity for internal audit to add even more value. Audit committees are also increasingly prioritizing compliance with laws and regulations, with more than one-third citing it as a top-three priority, a significant increase from last year.

CYBERSECURITY REMAINS NO. 1 PRIORITY FOR AUDIT COMMITTEES, FOLLOWED BY ERM

Cybersecurity topped the list of committee priorities by nearly 20 percentage points over ERM. Notably, 58% of respondents said the audit committee has primary oversight over cybersecurity, with 25% indicating the full board has oversight responsibility. Sixty-nine percent of respondents highlighted cybersecurity as a top concern in the next 12 months, with 3-in-10 ranking it No. 1.

The heightened focus on cybersecurity is likely due to greater disclosure requirements from regulatory agencies. The U.S. Securities and Exchange Commission (SEC), for example, is requiring new disclosures on cybersecurity risks and incidents, as well as management and strategy, including an explanation of oversight processes.

When considering what additional expertise would enhance the audit committee's effectiveness, cybersecurity was highlighted as the top area (44%). This is particularly notable given that almost half (48%) of respondents said they have some level of cybersecurity expertise on the committee.

The evolving risk landscape and emerging risks have put an increased spotlight on ERM. Nearly half of respondents indicated that ERM will be a top focus area in the next 12 months. More than three quarters (85%) of respondents reported some level of ERM expertise on the audit committee, positioning it to effectively oversee management's risk programs.

Learn more at deloitte.com.