TECHNOLOGY

BY TRACEY BIRKENHAUER

CYBER CATASTROPHE LOOMING?

BUSINESSES IGNORE DIGITAL DEFENSES AT THEIR OWN PERIL

As information security becomes a top priority for businesses, compliance has become a key driver of growth. In an era of escalating cyber threats, businesses are playing a dangerous game of Russian roulette with their data and network infrastructure.

Despite increasingly sophisticated cyber-attacks that can obliterate company assets overnight, most organizations are shockingly under-prepared, treating cybersecurity as an afterthought rather than a critical business imperative.

The landscape is evolving rapidly, with artificial intelligence serving as both a formidable threat and a vital defense in cybersecurity.

"Business disruption is a major risk," said Darrin Swan, Co-Founder and Vice President of Sales, Todyl. "The likelihood, the probability, is quite high—it's the highest it's ever been right now. We also know business email compromise (BEC) is the highest it's ever been in recorded history."

Based in Denver, Colo., Todyl is a cybersecurity firm that develops tools to help businesses identify and mitigate cyber risks, specifically detecting sophisticated threats like undetected server compromises and business email breaches that traditional security measures miss. Todyl sells its products and services to Managed Service Providers (MSPs), who provide outsourced IT services to companies around the globe.

In 2024, Todyl's Managed Extended Detection and Response (MXDR) team observed a 558% increase in adversary-in-the-middle (AiTM), account takeover (ATO), and business email attacks. Additionally, their digital detectives identified a suspicious access pattern from a small hosting provider targeting Microsoft 365 services.

Their efforts to search for threats not only improved their ability to detect unusual activities but also allowed the team to uncover a large network of identity attacks. This network included thousands of hosts across various regional and local Internet Service Providers (ISPs) in the U.S. and other countries.

"We found 5,000 servers operating in the United States of America for the last two years going undetected," Swan said. "Executing business email compromise at scale, unbeknownst to the users, and operating like you are not triggering all of the traditional security measures that would tell you that you got compromised.

"But we found it and nobody else did," Swan said. "It's what we do."

They discovered 37% of the known servers used by the threat group, which Todyl named the Söze Syndicate, are located in New Jersey. Additionally, 15% are in Germany and 9% in the United Kingdom. The remaining ISPs are distributed across New York, California, and Florida, as well as countries like France, The Netherlands, Norway, Switzerland, and Singapore.

Cyber Compliance Frameworks

Building and maintaining customer trust is critical for business success, especially as organizations increasingly require proof of strong data security practices from vendors and partners. Large enterprises, in particular, mandate compliance with industry standards such as Service Organization Control (SOC) 2, International Standards Organization (ISO) 27001, and National Institute of Standards and Technology Cybersecurity Framework (NIST CSF).

Many compliance frameworks demand robust cyberse-

curity measures, including password managers, Security Information and Event Management (SIEM) systems, 24/7 monitoring, IT change management, vendor risk assessments, and continuous employee cybersecurity awareness training.

"What matters most is the delivery to the customer to generate revenue, but in the middle is all the risk," Swan said. "If your system got all its data compromised, what would that do for your ability to deliver to your clients?"

Many of these clients, particularly in regulated industries such as finance, health care, and government, are increasingly requiring vendors to obtain and retain SOC 2 Type 2 (System and Organizations Control) compliance to ensure secure handling of sensitive data. For instance, banks and credit unions often mandate their service providers hold a SOC 2 Type 2 audit report to verify adherence to stringent data security standards.

Achieving SOC 2 Type 2 compliance is a rigorous process that requires companies to undergo months of auditing and continuous monitoring to ensure they meet strict security and operational standards. Many small and mid-sized businesses do not pursue it due to the cost and resource investment required.

Strategic Investment

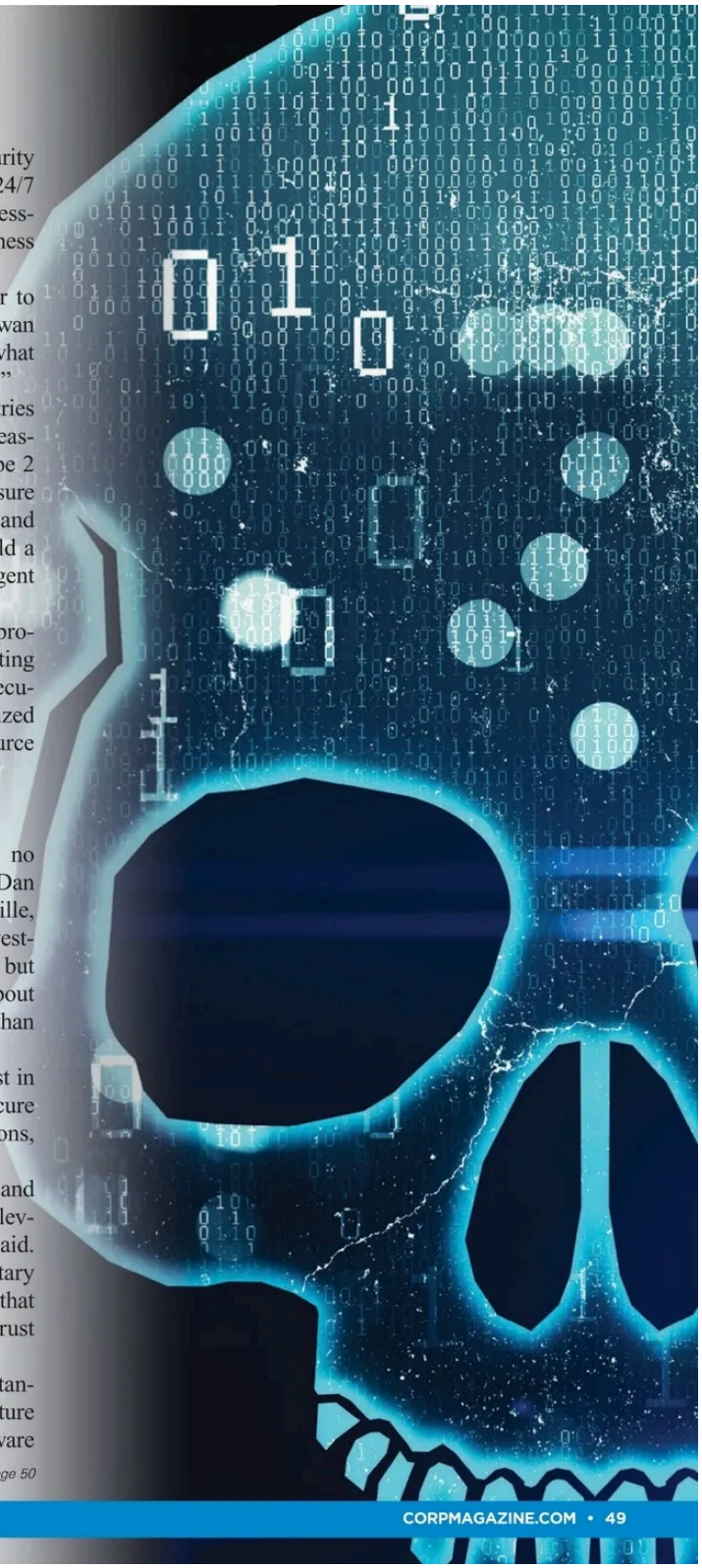
"In the digital economy of 2025, cybersecurity is no longer just a shield—it's a competitive advantage," said Dan Sitton, CEO of Guardian Technology Group in Jacksonville, Texas. "Businesses that treat security as a strategic investment, rather than an afterthought, will not only survive but thrive. It's not about preventing every breach—it's about building resilience to adapt, respond, and recover faster than the threats evolve."

Sitton's career began as a Tactical Network Specialist in the United States Marine Corps, where he managed secure communication networks under high-stakes conditions, honing discipline, precision, and technical expertise.

"I started Guardian Technology Group to help banks and credit unions move beyond basic compliance and truly leverage cybersecurity as a strategic advantage," Sitton said. "After years of safeguarding critical assets in the military and financial sectors, I saw a need for tailored solutions that not only protect institutions but also strengthen their trust and resilience in the eyes of their clients."

Critical infrastructure is now required to report substantial cyberattacks to the Cybersecurity and Infrastructure Security Agency (CISA) within 72 hours and ransomware

continued on page 50



payments within 24 hours. The Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA) provides CISA with greater visibility into cyberattacks for coordinated government responses and allows the agency to subpoena entities that do not report incidents. Organizations that fail to comply with the subpoena can be referred to the Department of Justice.

"This historic, new law will make major updates to our cybersecurity policy to ensure that, for the first time ever, every single critical infrastructure owner and operator in America is reporting cyberattacks and ransomware payments to the federal government," Sen. Gary Peters (D-Michigan) said shortly after the law was passed.

Trillion-Dollar Industry

Cybercrime has surged into a trillion-dollar global industry, fundamentally transformed by AI technologies that enhance how attackers infiltrate systems. Highly skilled hackers can now generate phishing emails in mere seconds, produce hyper-realistic deepfakes, and develop ransomware capable of analyzing vast datasets to refine their attack strategies. Research indicates that phishing continues to be the leading cyber threat.

"For many years, criminals have been investing billions of dollars into people, process, and technology," said Todd Thorson, Chief Technology Officer of TANJ Cybersecurity & Technologies in Yorkville, Ill. "Sadly, businesses have not kept up. Some larger businesses have hired proper experts, but that usually only happens after they have a breach.

Dan Sitton, CEO, Guardian Technology Group in Jacksonville, Texas.

"Criminals understand this and have shifted their targets away from Fortune 500, and to smaller businesses, as they are a much easier target," Thorson added. "AI has bolstered this effort, allowing fewer workers to target many businesses at once. Smaller paydays also keep them off the authorities' radar. With so many companies at risk, it is no wonder that every 39 seconds someone is losing money to criminals, and it amounts to $27 million per day out of our economy."

Insurance premiums, supply chain costs, and operational overhead are all increasing due to the growing threat of digital attacks.

Things Have Changed

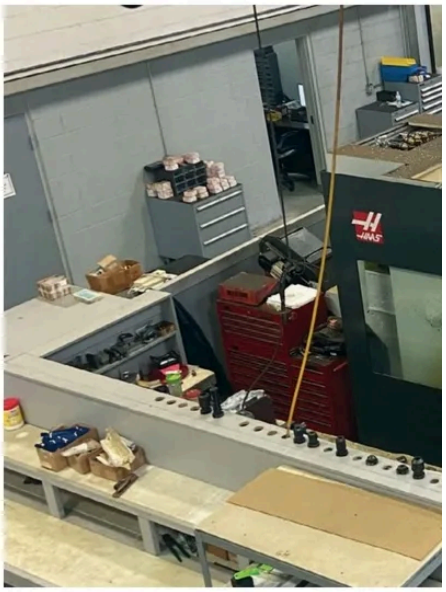
"I honestly would say Covid was the beginning of this cybersecurity change," said Jake Charen, Commercial Risk Architect at Lakeside Insurance in Broomfield, Colo., who specializes in business cybersecurity insurance. "So, everybody going remote for companies that required people to be in the office every single day, no matter what. Even if you had a cold or whatever, we were showing up to work as it used to be in 2019 or prior. Then once that happened, that's when the ransomware industry just completely changed.

"Hackers on the Dark Web were selling different types of ransomware kits. So, anyone could just buy it online and then pretty much hack into a company without having much experience. They were making whatever at first, up to $10,000, and then, somehow, these demands just drastically increased. Now it's like five hundred thousand or five million, right? I mean, they're just throwing ridiculous numbers."

Many remote employees went to the office just in time for the AI explosion.

AI has been developing for decades, with significant milestones in nearly every decade since the 1950s. However, its popularity surged dramatically in the 2010s and 2020s, particularly with the advent of machine learning and deep learning technologies.

The pandemic accelerated AI adoption as many organizations invested in AI to support remote work, enhance customer experiences, and reduce costs. This trend continued as staff returned to work, with AI playing a crucial role in adapting to new norms and improving operational efficiencies.



While AI was already on a growth trajectory, the pandemic significantly boosted its adoption and integration into everyday business practices.

"So, I think AI coming into effect has just completely changed what we need to view from a cybersecurity standpoint," Charen said. "It's not someone in Russia that can't speak English anymore, typing an email you can clearly tell is fictitious. Now, they'll just throw it into an AI tool, and it's gonna type it the right way. They can even get into your system and watch you and see how you like to do certain things and how your clients interact with you."

Charen says one of the biggest issues he experiences in his cybersecurity insurance practice is clients who parrot: "I'm too small."

"It's like, well, they're not just going after you," he added. "They're going after 500 businesses in your zip code and just hoping that one person clicks the link."

While Charen highlights the evolving threats posed by AI in cybersecurity, the conversation naturally shifts to the broader strategic considerations of cybersecurity investment.

Return on Investment

"Cybersecurity starts with business matur-

Like many government contractors, Taylor Turning in Wixom, Mich., is pursuing a cybersecurity certification to meet new cybersecurity requirements.

ity," said Chris Johnson, Senior Director of Cybersecurity Compliance Programs for the Global Technology Industry Association (GTIA), formerly known as CompTIA. "Governance, leadership, culture, and strategy are all common ingredients of success. Businesses that don't have leadership buy-in for information and network security will be reduced to just buying cybersecurity from a line card. For far too long businesses have looked at compliance (regulated or not) as a box to check and not something that gets embodied into their organization."

For modern businesses, the critical question has become a strategic calculation: how much financial investment will be dedicated to cybersecurity protection versus the financial risk of a potential breach? This is no longer an optional consideration but a fundamental business decision that requires careful economic analysis.

Team Sport

"Small businesses continue to be the backbone of America's economy, yet they are increasingly targeted by cybercriminals exploiting even the simplest security gaps," said Dave Alton, Chief Technology Officer at Strategic Information Resources, Inc. in Los Angeles, Calif. He also chairs the Global Cybersecurity Task Force for GTIA.

"Cybersecurity must be a team sport. If it isn't, it puts a strain on everyone that participates in the economy. It demands that every business, regardless of size, implements basic protective measures. The majority of cyberattacks are preventable with straightforward policies, training, and readily available technologies. By partnering with a Managed Service Provider as your guide, businesses can seamlessly integrate these defenses, ensuring a safer digital environment for all." The era when business leaders evaluated technology solely based on return on investment is behind us. Today, companies prioritize protecting their assets just as much as they focus on leveraging technology for growth.

"While MSSPs (Managed Security Service Providers) still have to do all the things we did 10 years ago to allow technology to enable the business, we now have to also use technology as a shield against cyber criminals," Thorson said. "The only item left to consider is, 'What will you do to protect your business now that you are aware of these risks?'

The Role of MSSPs

MSSPs have become the front line of digital protection. As Charen bluntly states, "It's not if you'll have a breach, it's when."

MSSPs leverage advanced AI-powered threat detection, offering real-time intelligence and rapid response capabilities that can mean the difference between a minor incident and a total system compromise. MSSPs also have highly trained security personnel on staff to recognize threats, hunt for threats, and provide their clients advanced cybersecurity protections.

"The cybersecurity landscape has evolved to a point where businesses need to be vigilant, 24x7, yet, they are not," said Rich Miller, CEO and founder of STACK Cybersecurity, an MSSP that recently transitioned from a traditional MSP. "A modern MSSP provides continuous protection through 24/7-monitored Security Operations Centers, Security Information and Event Management systems, and Managed Extended Detection and Response solutions. "These technologies allow us to detect, analyze, and neutralize threats before they can do damage. For organizations—especially DoD contractors—having this level of security isn't just a best practice, it's a necessity."

STACK Cybersecurity provides cybersecurity and outsourced technology services to clients nationwide, including those handling sensitive government contracts.

"The threat landscape changes daily," Miller added. "Businesses need a proactive security partner, not just an IT provider. That's where MSSPs come in—to offer expertise, technology, and round-the-clock monitoring that most businesses simply can't manage in-house."

More Education, Resources Needed

The future of cybersecurity resembles a perpetual arms race. Organizations are now required to adopt zero-trust architectures, invest in ongoing employee training, and stay nimble in response to ever-evolving threats. Network segmentation, comprehensive incident response planning, and fostering a culture of security awareness are just as essential as the most sophisticated technological defenses.

The National Cybersecurity Alliance "Cybersecurity Attitudes and Behaviors, Oh Behave! 2024-2025" report demonstrates many employers are moving in the wrong direction, as there's been a 56% decline in cybersecurity training access.

More than half of employed participants (52%) and students (58%) said they have not been trained to use AI safely. And 65% of respondents are concerned about AI-driven cyber risks. A concerning 38% admitted to

Some STACK Cybersecurity staff with Visit Detroit leaders in the cybersecurity firm's Livonia, Mich. office.

sharing sensitive work information with AI without their employer's knowledge. These AI-influenced transgressions are more prominent among younger generations (46% of Gen Z, 43% of Millennials).

"The growing concern about AI-related cybercrime reflects a heightened awareness of the digital threats we face," said Lisa Plaggemier, Executive Director of the National Cybersecurity Alliance. "However, with over half of participants (56%) not even using AI tools, and most (55%) of those using AI not being trained on the risks, it's evident that more education and resources are needed. We must continue to offer clear, practical guidance to help individuals understand and manage the risks associated with AI, ensuring they can protect themselves and their families in an increasingly digital world."

Critical Sectors Under Siege

The stakes have never been higher. Recent high-profile breaches, like the Department of Defense and Michigan Medicine's cybersecurity compromises, underscore the vulnerability of even the most secure systems.

These attacks have exposed critical weaknesses in national infrastructure, demonstrating how a single employee's momentary lapse can open doors to catastrophic data breaches.

The Department of Defense experienced a significant breach in April 2024. The attack targeted sensitive military systems and networks, with an emphasis on data exfiltration and espionage. The breach involved sophisticated tactics, including exploiting zero-day vulnerabilities and advanced social engineering techniques, which allowed hackers to gain unauthorized access to classified military information.

The breach led to concerns about national security, and while the full scope of the damage was still being assessed, the attack highlighted vulnerabilities within the DoD's IT infrastructure, particularly in relation to its supply chain and contractor networks. The incident led to an immediate investigation, increased cybersecurity measures, and a broader review of the DoD's cybersecurity posture.

The event underscored the growing threat to government and defense-related sectors as adversaries continue to target critical national security systems. The breach prompted a renewed focus on enhancing cybersecurity protocols across federal agencies, especially regarding the defense sector's complex supply chains.

In September 2024, Michigan Medicine suffered its second cybersecurity breach in four months. An employee inadvertently accepted an unsolicited multi-factor authentication (MFA) prompt, giving attackers access to their email account. The breach exposed protected health information, including names, medical record numbers and diagnostic details.

The breach, attributed to a targeted cyberattack, allowed unauthorized access to unclassified communications, potentially jeopardizing national security. The exposed information included sensitive data related to defense operations and personnel, underscoring the urgent need for enhanced cybersecurity measures to protect critical government infrastructure from future attacks.

"We need to have more accountability in this," Alton said. "This is an 'everyone' problem, not just infrastructure, mid-market or small businesses, and it isn't necessarily up to MSSPs or MSPs to keep clients safe. Everyone has to be doing this. If you aren't doing the basics, then you are part of the problem."

Manufacturing Cybersecurity Requirements

All DoD contractors are required to comply with the Defense Federal Acquisition Regulation Supplement (DFARS) minimum cybersecurity standards to maintain their federal contracts.

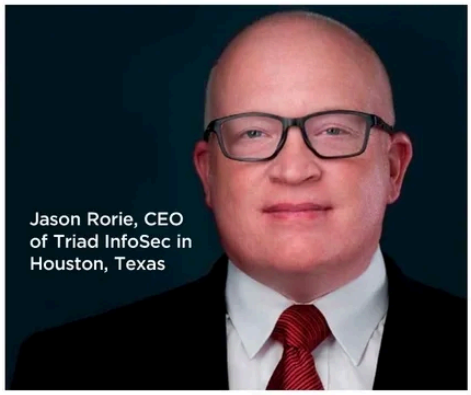
When Taylor Turning was founded 40 years ago in Wixom, Mich., cybersecurity wasn't a thing. As manufacturing has evolved and matured, so have the technology and risks.

Taylor Turning specializes in prototype and small-run production in the automotive and medical fields.

"Today, staying ahead means taking proactive steps to protect our business and future opportunities," said Ausstin Ritz, Accounting Manager, Taylor Turning. "Pursuing CMMC (Cybersecurity Maturity Model Certification) certification is part of that strategy—not just to prepare for potential government contracts, but to safeguard everything our founder built over the past four decades."

Running a small business means every

Lisa Plaggemier, Executive Director of the National Cybersecurity Alliance.


Jason Rorie, CEO of Triad InfoSec in Houston, Texas

decision counts, Ritz added, and Taylor Turning knew they couldn't manage this undertaking alone. They needed a team of experts to guide them toward compliance.

"That's why I partnered with STACK Cybersecurity," Ritz said. "They've helped us secure our systems, prepare for compliance, and identify threats that might not even be visible. Their expertise has given me peace of mind, knowing we're doing things the right way and staying ahead in an increasingly competitive industry."

This journey isn't just about protection; it's about staying competitive.

"In today's manufacturing world, cybersecurity isn't optional, it's a key differentiator," Ritz said. "Companies that fail to mitigate their cyber risk are falling behind, and I won't let that happen to Taylor Turning. With STACK's support, we're able to focus on delivering high-quality precision machining while safeguarding our reputation, protecting our customers, and securing the livelihoods of our team."

Weak Links Exposed

As traditional network boundaries dissolve, organizations are rapidly adapting. The convergence of operational and information technologies has created complex new attack surfaces. Internet of Things (IoT) devices, remote work environments, and cloud migrations have fundamentally reshaped cybersecurity strategies, demanding a more dynamic and intelligent approach to defense.

"Cybersecurity isn't just about technology—it's about safeguarding what keeps our nation running," said Jason Rorie, CEO of Triad InfoSec in Houston, Texas. "Critical infrastructure like defense systems and health care are prime targets for adversaries, and breaches like those at the DoD highlight the devastating consequences of weak links in the chain."

Rorie, a military veteran, sold his Managed Service Provider business to focus strictly on compliance. He holds multiple certifications that demonstrate his extensive expertise across various cybersecurity domains, including executive-level management, information systems auditing, cloud security, and compliance with the Cybersecurity Maturity Model Certification program. He's also a Cybersecurity Maturity Model Certification Certified Professional/Certified Assessor.

"I started my business to help organizations, from DoD contractors to corporations, move beyond compliance checklists and build real cyber resilience," Rorie said. "Compliance frameworks like CMMC are crucial for setting standards, but they're only a starting point. True security comes from embedding robust practices that adapt to evolving threats, protecting the systems we rely on most."

Compliance with Evolving Regulations

As we navigate this complex digital landscape, one thing has become crystal clear: cybersecurity is no longer just an IT problem. It's a critical national priority that demands collaboration, innovation, and unwavering vigilance.

Secureframe, a compliance software provider, surveyed over 160 small businesses to assess the financial impact of using a compliance management solution. The study explored cost savings, efficiency improvements, and overall ROI. Nearly half (47%) of small businesses reported having no dedicated compliance role before adopting automation, with an additional 33% sharing compliance responsibilities across multiple roles.

In such scenarios, compliance responsibilities often fall to operations or technology executives who often lack the time or knowledge to manage large-scale compliance projects. Most corporations leaning into makeshift security processes are prone to errors, increasing the risk of compliance issues, delays, and even failed audits.

Emphasizing cybersecurity as an integral part of compliance is essential to mitigate these risks and ensure robust protection against cyber threats.

Unable to demonstrate compliance, businesses risk losing revenue opportunities and existing clients. However, they often lack the resources to achieve compliance independently, especially within tight deadlines.

MSSPs can assist these companies by identifying relevant frameworks and standards and aligning them with their strategic goals. Additionally, automating compliance processes enables these businesses to meet requirements swiftly and efficiently.

Looking Ahead: Emerging Trends and Best Practices

Moving further into 2025, several trends are emerging in the cybersecurity landscape:

1. Increased state-sponsored attacks targeting critical infrastructure
2. More sophisticated attack methods, including AI-driven threats
3. Growing risks associated with Internet of Things (IoT) devices and cloud migration in critical systems

To mitigate these risks, organizations must prioritize cybersecurity measures such as:

- Network segmentation to limit the spread of potential breaches
- Regular security testing to identify and address vulnerabilities
- Adoption of zero-trust principles to enhance overall security posture
- Implementation of robust incident response plans to minimize damage from successful attacks
- Continuous employee training to create a security-aware culture

The lessons learned from recent high-profile attacks emphasize the need for proactive threat intelligence and the ability to rapidly adapt to new threats as they emerge.

As cyber threats continue to evolve at an unprecedented pace, the protection of critical infrastructure remains a top priority for national security and public safety. The integration of AI into both offensive and defensive cybersecurity measures has raised the stakes, making it more crucial than ever for organizations to remain vigilant and adaptive in their security strategies.

The battle for digital security has only just begun.