Mike Sanchez, CISO and SVP of cybersecurity solutions at UDT. Courtesy photo

COMMENTARY

2024 Will Test Cybersecurity Leaders: Is Your Company Ready?

Experts say new AI-driven threats and an election year will spell trouble for companies.

April 24, 2024 at 12:04 PM

7 minute read

Board of Contributors

By Mike Sanchez | April 24, 2024 at 12:04 PM

In my daily work as a chief information security officer helping business leaders in South Florida and across the country, I recognize that keeping up with the ever-changing and evolving cyber threats is becoming increasingly challenging and stressful for companies. History has proved that what can sometimes be a natural reaction for companies—digging their heads in the sand and hoping the threats disappear—is not a luxury that anyone can continue to afford. The stakes are too high and the consequences are too severe.

UDT's sophisticated threat intelligence insights show that 2024 could be a cyber nightmare across industries. Here are the two primary reasons:

- **Generative AI:** Artificial intelligence is a powerful tool with the capacity to do a lot of good, but it can also be easily exploited. Hackers are already using the accelerated adoption of generative AI to create realistic and convincing phishing emails, fake videos and deepfakes that can trick users. AI can also provide specific instructions on how best to bypass security systems and gather stolen information, empowering cybercriminals to automate and scale cyberattacks more efficiently while making them harder to detect.
- **Election Year:** Several of the world's most populous countries are hosting elections this year, including the United States. This makes them targets for cyber interference and influence campaigns, as well as phishing and ransomware attacks that can disrupt the voting process and undermine public trust. Cybercriminals will seek to disrupt operations and cause delays, alter information where possible, and corrupt systems. Compromised user accounts will be leveraged to send out misinformation and disinformation, and gain access to other systems tied to voting systems due to weak network segmentation.

While 2024 could be a rough year for cybersecurity, there are actions you can take to prepare and protect your organization. Based on our experience, here are the top five questions that C-suite executives should ask their top security leaders to address:

First, it is important to note that CISOs have a huge responsibility to protect their organizations from cyber threats, and to ensure they have the right strategies, tools, and processes in place to prevent, detect, and respond to incidents. To help assess a company's readiness and security posture, there are five fundamental questions to consider:

- **"Have I already been hit with an attack but don't know it yet?"** Many cyberattacks are stealthy and can remain undetected for months or even years while attackers exfiltrate data, compromise systems, and prepare for the final blow. You need to deploy a proactive approach to hunt for any signs of compromise and to remediate any vulnerabilities before they become a breach.
- **"Are the right protections and policies in place to make it difficult for bad actors to successfully target the organization?"** Technology alone cannot solve security problems. Companies need to adopt a zero-trust and risk-first philosophy alongside a robust and layered defense that covers all their assets—from endpoints to networks, cloud to on-premises, users to applications. A strong security culture is required to educate employees on ways to be vigilant and responsible. Also critical: a comprehensive and updated security policy that aligns with the company's business objectives and compliance requirements.
- **"How can we determine whether any of our users' information has been compromised and made available for purchase?"** Hackers sell and buy stolen data on the dark web. Companies need reliable visibility into the dark web to understand what credentials and access may have been compromised. They need to have a way to monitor and alert on any exposure of their sensitive information, and to take action to mitigate the impact and prevent further damage.
- **"What specific detection rules should be in place to help ensure that the attack vectors being used are *really* being caught and remediated?"** A dynamic and adaptive detection system is required to keep up with the ever-changing and sophisticated tactics, techniques, and procedures (TTPs) of cybercriminals. It's important to have a correlation and analysis engine that can accurately identify and prioritize the most relevant and critical alerts while reducing noise and false positives. It is critical to also have a response and remediation plan in place to quickly, effectively contain and eradicate threats, then restore normal operations.
- **"How can we know if there are hidden rules in email platforms that send copies of emails to be sent to unrecognized parties?"** It is important to have a control and audit mechanism that can detect and prevent any unauthorized or malicious changes to email settings, such as forwarding rules, inbox rules, or transport rules. An appropriate verification and validation process is also important to ensure that email communications are secure and authentic.

For many companies, answering these questions can often feel daunting and overwhelming. Cybersecurity is a highly specialized area. Many companies lack the time, resources and expertise to answer them on their own. Smart business leaders are relying on expert partners who can be responsible for managing these headaches and advise them on the best solutions for their specific needs and challenges.

Mitigate Risk by Knowing Where to Act First

Staying vigilant and proactive is important in the face of rising cyber threats, especially for companies that don't feel as confident in their security posture after answering the above questions. The first step is to strategically address the risk by gaining visibility into the current environment.

There are a variety of assessments available to test and assist in providing insights and feedback into cybersecurity measures. Here are a few to consider:

- **Compromise Threat Assessment:** This assessment can help reveal any current or past compromise in the environment, providing a detailed report and actionable recommendations on how to improve security posture.
- **Ransomware Readiness Assessment:** This assessment can help evaluate resilience against a potential ransomware attack. Combining this assessment with a tabletop exercise enables companies to take a more focused approach, leveraging simulated scenarios to test their response capabilities and identify any gaps or weaknesses.
- **O365 Resiliency Assessment:** This assessment enables companies to secure their O365 environment by performing a comprehensive assessment of their settings, policies, and configurations, then providing them with best practices and recommendations on how to enhance their security and compliance.
- **Network and Website Application Penetration Testing:** This test mimics the real-world attack techniques used by the bad guys to assess networks and web application security. The result is a comprehensive report and remediation guidance.
- **Active Directory Resiliency Test:** This test can help companies secure their Active Directory, which is the crown jewel for any bad actor. Testing can identify any misconfigurations, vulnerabilities, or weaknesses that can expose an AD to compromise.
- **Dark Web Intelligence Scan:** This type of scan can help flush out compromised information that is available for purchase on the dark web. It enables companies to monitor for alerts on any exposure of their sensitive information so they can take action.
- **Offensive Security Assessment:** This assessment tests detection and response capabilities by performing a simulated attack. It provides feedback and a plan for optimizing security operations.

2024 may be the year of unprecedented cyberattacks, but with the right preparation, it doesn't have to be the year your company falls victim. Partnering with the right experts and developing a customized approach for your ecosystem can help you gain a significant competitive advantage—and priceless peace of mind.

Mike Sanchez, *CISO and SVP of cybersecurity solutions at UDT, a technology solutions provider that modernizes, secures, and manages complete IT systems for commercial enterprises, state and local governments, and education organizations. Sanchez may be reached at msanchez@udtonline.com.*

NOT FOR REPRINT
© 2024 ALM Global, LLC, All Rights Reserved. Request academic re-use from www.copyright.com. All other uses, submit a request to asset-and-logo-licensing@alm.com. For more information visit Asset & Logo Licensing.

TRENDING STORIES

Cravath Moves Into New Manhattan Headquarters
THE AMERICAN LAWYER

Sidley Austin's Scott Kilburg, 'Client-Focused' CMO, Dies at 51
THE AMERICAN LAWYER

Some Clients Are Pushing for Transparency Surrounding Origination Credits
THE AMERICAN LAWYER

Mayer Brown Set to Split With 170-Lawyer Greater China Offices
INTERNATIONAL EDITION

'A Legend': Paul Weiss Partner Michael Gertzman Dies at 60
THE AMERICAN LAWYER

LAW.COM PRO

People, Places & Profits, Part III: Are Law Firm Financial Metrics Keeping Pace With Inflationary Growth?

People, Places & Profits, Part II: A Look at the Geographic Destinations of the Am Law 200

A Tragic Death: How Should Big Law Respond to the Industry's Mental Health Crisis?

FEATURED FIRMS

Law Offices of Gary Martin Hays & Associates P.C.
(470) 294-1674

Law Offices of Mark E. Salomone
(857) 444-6468

Smith & Hassler
(713) 739-1250