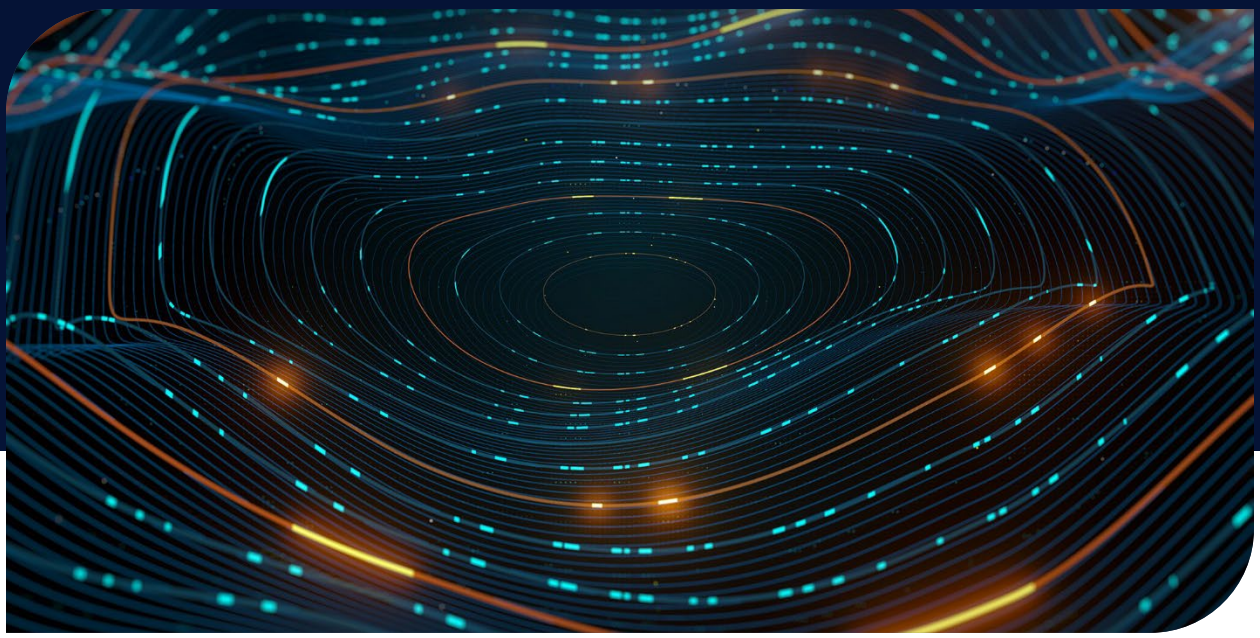
Teneo

Cybersecurity Insights:

Six topics leading the C-suite cybersecurity agenda in 2024

April 2024



Around the world, 2024 has already shown us that cybersecurity risk is alive and well.

In the U.S., highly disruptive attacks, targeting Microsoft, UnitedHealth Group and its subsidiary Change Healthcare, have cast a new spotlight on companies and their cybersecurity practices by not just customers, media and investors, but federal agencies and regulators. As of this writing, Change Healthcare is still digging itself out of a massive insurance claims backlog, and hundreds of thousands of providers and patients alike have been impacted. In a somewhat ironic twist, Microsoft itself reports that roughly 87% of UK organizations are vulnerable to a cyber-attack. In Europe, government entities and NGOs are tracking widespread phishing attempts by a likely Russian criminal gang which coerces employees into clicking on links and downloading malware. And across the Middle East, Africa and Asia, cyber criminals using ransomware are targeting organizations which they identify as potentially less mature in cybersecurity controls, made significantly more vulnerable as certain regions and countries across MENA still haven't appropriately prioritized or invested in cybersecurity.

Teneo

Cyber risk is here to stay. Operating despite this dynamic is a matter of how governments, NGOs and private sector entities track new developments, educate themselves and constituents on cyber risk, and most importantly, approach the concept of resilience. In the cybersphere, AI and ransomware are dominating headlines, but there are subtle nuances to these stories that are likely indicators of more threats to come.

The following brief is a summary of the executive cyber agenda issues we are tracking for 2024, and considerations for global businesses to address cyber risk by leading with intelligence, training and preparedness.

What Are We Tracking?

1. AI to cause harm: Generative AI like ChatGPT has been a gift for cybercriminals, and they have openly embraced the technology to cause harm.

While startups and major global organizations around the world celebrate the transformational benefits of AI implementation and AI market entrants launch new products and services for good, threat actors are similarly benefitting from advances in AI to cause harm. Generative AI tools like ChatGPT have reduced the time to market for malicious code to mere seconds, including creation of similarly disruptive tools such as deepfakes or phishing malware intended to cause financial or reputational harm. With virtually every piece of media available on the Internet, criminals are taking advantage of AI tools and code – many of which are traded on the cheap on the dark web – to create seemingly authentic audio and video to socially engineer victims. Unfortunately, the advances in AI and machine learning have a dark side – the gap in ability to discern between real and fake is quickly closing.

Empowered by AI and emboldened through espionage, IP theft, significant criminal funding and the anonymous shield of the dark web, nation-state actors such as Russia, China, North Korea and Iran have been able to quickly organize, build capabilities, execute cyber-attacks and disappear, only to re-emerge and reorganize – often evading law enforcement detection. Even though agencies such as the FBI, Interpol and the ACSC (Australian Cyber Security Centre) have made strides in more proactive detection, response and investigation, the complexity of the cyber threat landscape has unfortunately enabled the bad guys to stay one step ahead. To highlight that point, in early 2023, FBI Director Christopher Wray warned that Chinese cyber threat actors outnumber FBI investigators fifty to one – even if he were to put all of his available FBI agent attention solely on China. At the same time, cybersecurity leaders are also leveraging AI as part of their cyber strategy (for good!), with artificial intelligence capabilities enabling security managers to identify anomalies and combat threats at scale.

2. Disinformation and distraction: Geopolitics, elections and major 2024 global events offer significant criminal opportunities for the bad guys.

Concern over the spread of disinformation has taken center stage in a historical global election year where at least 64 countries will take to the polls. In the EU, the European Commission is set to adopt new regulation as early as April to promote election integrity through the teeth of the Digital Services Act (DSA). The Commission plans to issue fines to social media platforms such as X and Meta for failure to adequately moderate AI generated disinformation. As part of proposed regulation, platforms will be expected to organize dedicated teams to work with cybersecurity agencies across the EU's 27 member states in monitoring for problematic content.

In February of this year, the U.S. launched a bi-partisan task force to assess the potential for AI regulation, but with the U.S. presidential election just seven months away, it is unclear whether appropriate regulation will be in place which mirrors efforts by EU's DSA. Around the world, governments in Australia, Canada and countries across the Middle East and Asia are grappling with similar concerns; namely, how to hold social media platforms accountable. Cyber threat actors reap the benefits in the interim while regulation chases advances in the technology. Both public and private sector organizations are focused on preparing for potential administration changes in their respective geographies and assessing impact to domestic and global trade, economic policy, national security, energy and climate policies and international relations with two wars raging. In addition to elections, major global sporting events and the Paris 2024 Olympics create additional opportunities for threat actors to capitalize on what may feel like distractions – betting on finding vulnerabilities as businesses and other organizations try to prioritize and balance a full plate of activity.

3. Ransomware, but "as-a-service" (RaaS): Global regulation and increasing corporate resolve against ransomware payments will force threat actors to change strategy.

Ask most CEOs and C-suite executives what keeps them up at night, and they will likely express deep concern over the potential for a ransomware attack, if they haven't already dealt with one. The advances in AI propelling threat actor capabilities only deepen that concern, but evolving regulation may start to have a dampening effect on how far cyber criminals can push for ransom, not to mention that many global CEOs are digging in their heels and, on principle, won't pay.

In the last several years, more and more companies faced significant disruption and extortion at the hands of attackers, and companies felt they had no choice but to pay ransom to minimize impact to the business. As a result, these bad actors realized they were on to something and evolved ransomware attacks into a commercial operation. Foreign adversary criminal gangs set up call centers with English-speaking support desk help and streamlined the ransom payment process to quickly bank the revenue and move on to the next victim. At the same time, ransomware syndicates sprouted up, creating a network of code developers and attackers (think producers and distribution channels) to expand the global business operation.

That may be changing.

In October of last year, the U.S.-led Counter Ransomware Initiative, an organization of 50 member countries, pledged to sign an international agreement not to pay ransom demands. Further, global private sector businesses have increasingly and publicly declared they would not pay ransom – even in high-pressure, high-profile cyber-attack situations. Also in October, in the wake of a financially and operationally destabilizing attack on MGM Resorts International, CEO Bill Hornbuckle described the attack as "corporate terrorism," noting they elected not to pay ransom as part of recovery from the incident, and that they, rather, focused on investing in infrastructure, people and processes. Elsewhere, global law enforcement agencies have made strides in combating cyber criminals. In January, the FBI announced they had shut down Chinese criminal gang Volt Typhoon, and in February, together with the UK Crime Agency and Ukrainian law enforcement, shut down one of the most notorious and successful Russian RaaS networks, Lockbit, known for victimizing organizations like Boeing and the UK Ministry of Defense. And on March 25th, the U.S. and UK governments announced they had issued sanctions and charges against alleged Chinese hackers for espionage and targeted cyber-attacks against critical infrastructure.

The conundrum with paying ransom is that it alleviates a short-term problem while signaling to threat actors that a company has the resources to pay, and companies are feeling it. A 2024 study by Cybereason highlighted that 84% of companies hit with ransomware paid the ransom, yet 78% were then breached again, and 63% of these were asked to pay more the second time.

With global solidarity against paying ransom, law enforcement successes and the stark realization by organizations that payment is fueling further attack, the tide may be turning against large scale, lucrative RaaS endeavors. Expect to see threat actors changing tactics and strategies from the current service model to new ways of targeting organizations, and likely with AI. As noted previously, driven by anonymity, the bad guys have ways of disappearing, rebooting, retooling and reappearing in unfortunate, creative ways. For example, Sophos reported in December that criminal gangs are becoming increasingly media savvy and have built new strategies around engaging with reporters, providing FAQs and even interviews, all in the name of putting pressure on victims while generating buzz, attention and intrigue around themselves as hackers and their operations.

4. Insider risk: Whether they mean to or not, employees continue to be a primary source of cybersecurity risk.

By now, most managers overseeing employees and broader teams have heard the terms "unwitting" or "malicious insider" – respectively, employees who create cybersecurity risk either by mistake / through human error, or those that purposefully cause harm by disrupting operations, committing theft or attempting to cause reputational damage. Inattention, laziness and distraction are the usual culprits for those unwitting employees, but events such as corporate layoffs, financial motivation or discontent tend to be the impetus behind malicious insider activity. While experts point to remote or hybrid work as a reason for an increase in

insider risk since the pandemic, cybersecurity product companies have been quick to build new detection services to address a distributed workforce, and many corporate IT teams have implemented these services to enable a mostly here-to-stay remote work or hybrid work environment.

Yet, insider risk persists.

Enter the challenges with AI yet again. Code42, an insider risk management software development company, issued its 2024 Data Exposure Report with a particular focus this year on data leakage attributed to AI. The report highlights the following key statistics:

- 85% of cybersecurity leaders are concerned that their company's sensitive data is increasingly vulnerable to new AI technologies;
- 86% of cybersecurity leaders worry that employees may put sensitive data into GenAI that will be found by competitors.

Younger generations in today's workforce have been dubbed "digital natives," and the blurred line between work and personal devices for always on, always connected employees creates additional challenges in keeping company data secured. Despite their relative digital savviness, a Deloitte 2023 Connected Consumer survey reported that Gen Z is three times more likely to fall victim to phishing attempts or fraud scams than Baby Boomers. While that statistic may not exactly represent the norm, catering to and securing a multi-generational workforce with broadly diverse work habits and cybersecurity practices requires layers and flexibility.

5. **Executive and board director vulnerability: C-suite executives and directors are targets of opportunity for cyber-attack, mainly because of their access to highly sensitive data and perceived ability or resources available to pay ransom.**

An unfortunate by-product of an elevated profile, visibility and authority is elevated risk. Cyber criminals are well aware of the fact that C-suite executives and board directors have access to the most confidential and proprietary information associated with the firms they run – potentially putting these individuals at the center of ransomware and extortion tactics. In 2021-2023, we saw a spate of incidents where bad actors would "lock and steal" the data for ransom and then threaten to "publish" unless ransom was paid.

While company senior executives are under the information security supervision of their IT departments, and presumably as, if not more, secure than the rest of the employee base, they are likely also working from a home office (if not several) and accessing important company information either remotely or bringing it home with them on a company device into a personal home network. Board directors are in a similar situation, but often are not under the same information technology rigor as the employees of the firms they serve. Not all companies have instituted secure sites for director data access, leaving these individuals potentially vulnerable to intrusions. The bad guys can find it even more compelling to target board directors, given many serve on multiple boards, thus creating a federated access point to victimize multiple

organizations. Even worse, threat actors are known to move laterally to family members as another means of intrusion, buying personal information from data brokers on the dark web, including compromised social media account logins and other sensitive information that can be used to hack or scam the executives and / or family members into downloading malware or other infectious code, compromising personal home networks and email accounts.

Cybersecurity and data privacy firm BlackCloak, which provides services to executives and UHNW clients, conducted a 2022 assessment of member compromised data and reported that of their 1,000 members, many of which are Fortune 1000 company executives:

- 99% of their executives had personal information available on more than three dozen online data broker websites, with many listed on more than 100 sites;
- 70% of executive profiles found on data broker websites contained personal social media information and photos from sites like LinkedIn and Facebook;
- 40% of online data brokers had the IP address of an executive's home network.

Hopefully, since the 2022 insights from BlackCloak, corporations, executives and board directors have increased their level of awareness and have embraced improved cybersecurity measures to diffuse these vulnerabilities. The reality is, new board and C-suite level appointments are happening every day, and the threats and tactics targeting high-profile individuals are continually evolving. This means ongoing vigilance, intelligence and deliberate training on the cybersecurity risk will need to become part of the job description for these roles.

6. Onerous regulatory requirements: Global governments and regulatory agencies are rolling out strict regulatory reporting requirements for businesses and stepping up the focus on management and board accountability for cybersecurity.

A quick tour around the world from the U.S. to Europe and over to the Middle East and Australia highlights just how serious the cyber threat has become and underscores the growing importance of regulation on the topic of cybersecurity risk management.

On December 18, 2023, the U.S. Securities and Exchange Commission (SEC) began requiring public companies to disclose how they manage cyber risk (including how they assess threats and their potential impact) in their 10-Ks, as well as requiring companies to report any cyber intrusions that are likely to have a material impact on the company's operations to the SEC within four business days. The new reporting framework also places greater emphasis on the disclosure of board oversight related to cyber risks and the importance of crisis planning and communications in the event of cyber breaches.

In Europe, the new cybersecurity regulation issued on January 7, 2024, defines measures for the establishment of an internal cybersecurity risk management, governance and control framework for each Union entity, and sets up a new Interinstitutional Cybersecurity Board (IICB) to monitor and support its implementation by Union entities. On March 14 of this year, the Cyber Resilience Act was approved by the European Parliament, which outlines the legal framework

describing cybersecurity requirements for hardware and software products with digital elements placed on the market of the European Union.

In the Middle East, Saudi Arabia has issued a number of regulations such as the Personal Data Protection Law 2023, and the UAE and Jordan have recently passed regulation which outlines strict penalties and jail time follow any criminal activity associated with cyber-attacks. In Australia, a new Risk Management Protocol signed off by Minister O'Neil in February 2023 will make board members liable for failing to properly secure assets, covering companies across critical infrastructure sectors.

Cybersecurity regulation and the latest rollout of rules around the world by governments are a direct response to recent and high-profile cyber incidents which caused not only significant disruption and financial losses, but also highlighted the potential vulnerabilities in their respective homelands' security.

Considerations for Executives

Cyber intelligence in support of resilience

Executives are inundated with company data and metrics, analyst and expert reports, news stories and social media highlighting cyber risk. Staying on top of it all can be extraordinarily daunting. It is a significant and, frankly, fruitless endeavor to try to document and track every potential threat that may have some impact to business operations, employees, constituents and brand. Instead, C-suite executives and directors should discuss and assess the short-list of critical company assets that make or break the business and ensure a fulsome understanding of the risk tolerance for disruption of those assets and the relevant mitigation strategies to protect them.

With the range of threats highlighted in this brief, digital intelligence and threat monitoring calibrated toward proactive identification of potential risk to those critical assets helps narrow the analysis and provides focus for executive risk oversight. Cybersecurity spend and initiatives at the direction of the C-suite should be focused on building and achieving *resilience* – not simply security *protections*.

Preparedness and testing

The moment of a cybersecurity crisis is not the time to develop a crisis management plan. The threat landscape has likely changed dramatically since the last time an executive team dealt with a major disruption to the organization, and with the new issues related to AI and cyber risk, disinformation, evolving threat actor tactics and new regulation, now is the time to dust off the old plans if they exist, or develop and implement the appropriate crisis management strategy. It is important to note that crisis management and crisis communications are two different things – one defines "crisis" for the organization, as well as the means by which and when executive

management comes together to respond to a crisis, and the second defines the communications protocols to manage the crisis. Once the executive team has the crisis management and crisis communications frameworks in place, it is necessary to test those plans through table-top exercises or crisis simulation exercises to build muscle memory and ensure teams are not working through it for the first time during a live event.

Training

Humans (as evidenced by the commentary is this brief related to insider risk and high-profile executives and directors) are at the center of strong corporate cybersecurity – and risk. Education, awareness and ongoing corporate-mandated training on best practices to better identify suspicious activity and reduce vulnerability will be critical to protecting employees, their families and the organization. Regular review of executive and director digital exposure, coupled with removal of sensitive online information and simple changes to online practices, will go a long way in shoring up the risks potentially facing key leaders.

For more information, email: Resilience&Intelligence@teneo.com

Author

Courtney Adante
President, Security Risk Advisory
Courtney.Adante@teneo.com

Teneo
The Global CEO Advisory Firm

Teneo is the global CEO advisory firm.

We partner with our clients globally to do great things for a better future.

Drawing upon our global team and expansive network of senior advisors, we provide advisory services across our five business segments on a stand-alone or fully integrated basis to help our clients solve complex business challenges. Our clients include a significant number of the Fortune 100 and FTSE 100, as well as other corporations, financial institutions and organizations.

Our full range of advisory services includes strategic communications, investor relations, financial transactions and restructuring, management consulting, physical and cyber risk, organizational design, board and executive search, geopolitics and government affairs, corporate governance, ESG and DE&I.

The firm has more than 1,600 employees located in 40+ offices around the world.

teneo.com