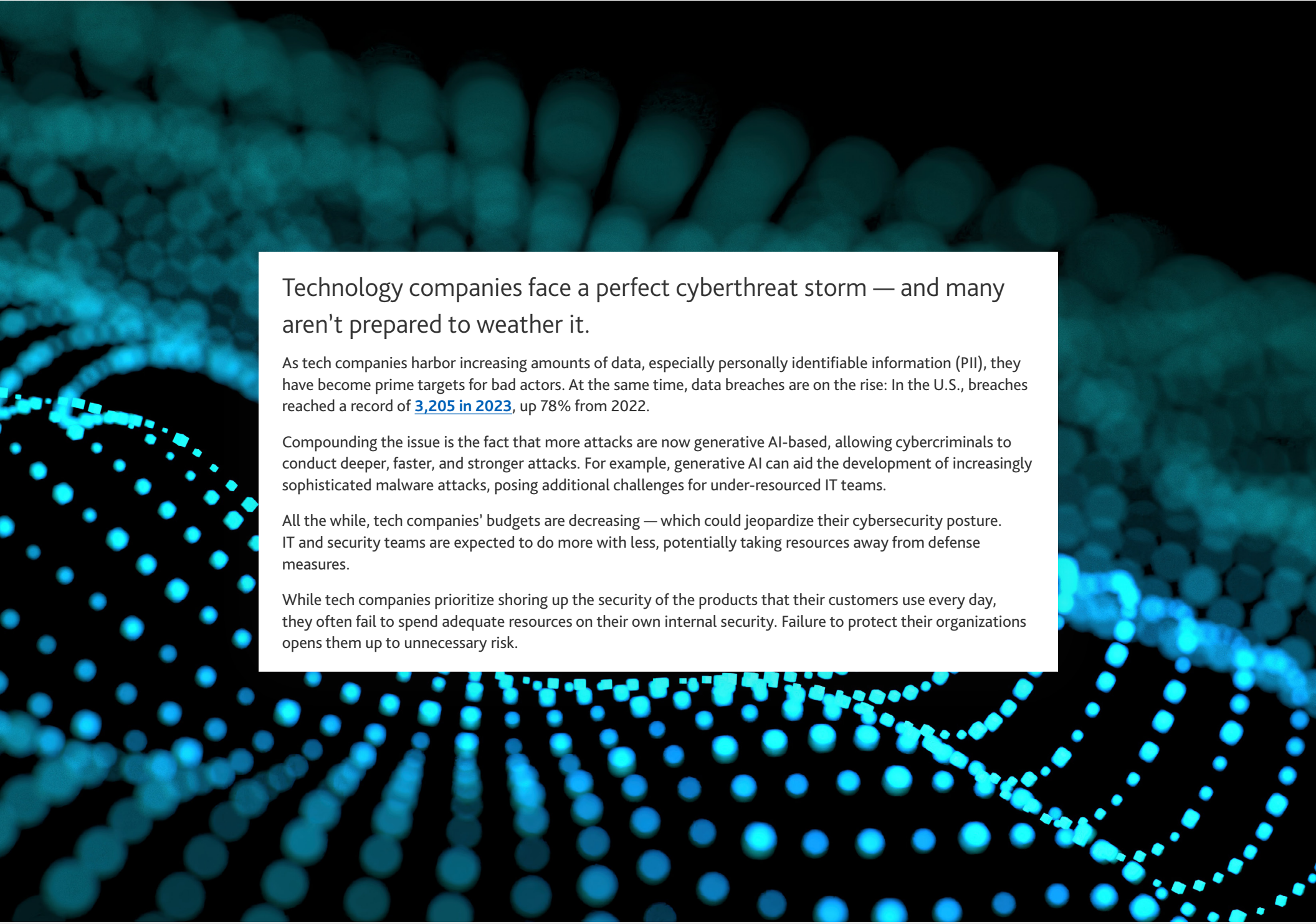
Addressing the Tech Cyberthreat Landscape

BDO



Technology companies face a perfect cyberthreat storm — and many aren't prepared to weather it.

As tech companies harbor increasing amounts of data, especially personally identifiable information (PII), they have become prime targets for bad actors. At the same time, data breaches are on the rise: In the U.S., breaches reached a record of **3,205 in 2023**, up 78% from 2022.

Compounding the issue is the fact that more attacks are now generative AI-based, allowing cybercriminals to conduct deeper, faster, and stronger attacks. For example, generative AI can aid the development of increasingly sophisticated malware attacks, posing additional challenges for under-resourced IT teams.

All the while, tech companies' budgets are decreasing — which could jeopardize their cybersecurity posture. IT and security teams are expected to do more with less, potentially taking resources away from defense measures.

While tech companies prioritize shoring up the security of the products that their customers use every day, they often fail to spend adequate resources on their own internal security. Failure to protect their organizations opens them up to unnecessary risk.

Tech's Top Cyber Risks

Generative AI is powering more stealthy attacks and at a higher volume than seen in previous years. Along with using generative AI to help create more advanced malware, it can also allow threat actors to examine stolen data much faster and on a larger scale. It can even power web scraping attacks that mimic human behavior while gathering code and data at incredible speed.

On the dark web, cyber criminals can also purchase Ransomware-as-a-Service (RaaS). RaaS offers pre-written codes to conduct attacks, meaning cyber criminals no longer need to be as technologically skilled, making hacking more accessible than ever before.

Another major risk that tech companies face is a lack of understanding and awareness of the gaps or vulnerabilities that exist within their own internal systems and technologies. Tech companies often overlook weaknesses within their organizations and fail to understand what data is at risk, where it lives, and who has access to it. These gaps could be due to a lack of internal education, resources, budget, or a combination of all three. Moreover, IT teams with reduced budgets and limited cybersecurity training may lack the means necessary to address known risks or strengthen data security.

Because the cyber risk landscape is increasingly complex, internal IT teams face an uphill battle when reporting cyber risks to the board. They may struggle to quantify risk and illustrate the ROI for increasing cybersecurity investment. The result: The board does not grant additional funds to bolster cyber defenses.

Many tech companies also face significant third-party cyber risk. Working with vendors increases connectivity between organizations, which can in turn increase access points for threat actors. To protect their systems and sensitive data, tech companies must thoroughly assess vendors' cybersecurity practices and identify potential vulnerabilities. It is paramount that IT teams put processes in place for third-party vetting and risk mitigation, as protecting sensitive data is the responsibility of all parties. At the same time, these security protocols shouldn't be so onerous that they impede the ability of third parties to complete their work.

To find the right balance when developing security protocols, companies should focus on protecting their "crown jewels." What's the most important data to protect? What data is most valuable to threat actors? Which vendors have access to it? Start by answering these questions to identify the "jewels" and then layer defense around that data internally and with third parties.

Understanding the SEC's New Cybersecurity Disclosure Rules

The Securities and Exchange Commission's (SEC) new cybersecurity disclosure rules present challenges for tech companies. These rules mandate that companies determine the materiality of a breach within four business days — an extremely short window for organizations suffering from a data breach.

To comply with the SEC's new rules, tech companies must first get their data house in order. A strong cybersecurity posture is predicated on sound data governance, data management controls, and a deep understanding of how data flows within a given organization. Tech companies will then need to create a strong incident response (IR) plan with supporting documentation in case of a breach. Companies will find it difficult to swiftly analyze and disclose the breach if their IR plans are incomplete, or their documentation is incorrect.

The SEC is putting pressure on corporate boards and their management teams to strengthen their processes and governance internally to comply with the new rule. It's reasonable to assume that companies will soon be expected to move beyond defensive measures and adopt a proactive stance for timely detection and reporting.

Improving Your Cybersecurity Posture

Tech companies must strengthen their cybersecurity posture to adapt to the evolving threat landscape. Fortunately, there are many steps tech leaders can take:

1. Reinforce Data Governance

A strong data foundation is important for defending against cyber threats and meeting regulatory requirements. Consider reassessing where data resides, internal access privileges, data retention policies, data transferring processes, reporting mechanisms, and more. Data governance and data security are inextricably linked, so enhancing one benefits the other.

2. Create a Culture of Compliance

Organizations should deploy ongoing training, upskilling, and internal education to make employees aware of shifting threat tactics. Employee education should be the first line of defense against cyberattacks since most breaches prey on employee error. Basic security hygiene, such as teaching employees to regularly update their systems and enable multi-factor authentication, can go a long way: 98% of attacks can be prevented with good cyber hygiene. Part of creating a vigilant culture may also mean appointing cybersecurity leadership, such as a Chief Cybersecurity Officer.

3. Adopt a Zero Trust Framework

This concept treats every attempt to access the organization's systems as a potential threat and only grants entry after verification, minimizing data access. Zero trust frameworks can reduce the chance of a data breach by 50%. Improving cybersecurity protocols and policies is easier when starting with a zero trust framework, as opposed to more robust and rigid frameworks like that of the National Institute of Standards and Technology (NIST).

4. Use a Layered Defense Model

This model hinges on using multiple types of security measures — or layered measures — so that if one fails, there are other lines of defense to identify, prevent, or slow down the attack. By implementing multiple controls around the most vulnerable areas, a company increases its chances of stopping an attack in its tracks.

5. Leverage Threat Monitoring and Intelligence

Ongoing threat monitoring screens the threat landscape to detect nefarious activity, while using detailed industry-specific threat intelligence helps organizations arm their teams with distinct, actionable information in the face of an attack.

6. Validate Security Defenses

Companies should conduct regular penetration testing and other tabletop exercises to proactively identify and address potential weaknesses.

7. Strengthen IR Plans

Data breach response and reporting processes should be formalized in accordance with emerging regulations such as the SEC's new cybersecurity rules. Defensive measures, such as putting up safeguards to keep attackers out, are likely no longer enough. Companies should assume attackers can get in — or have already been in — and have robust processes in place to react to and report on a breach as soon as possible. Many organizations have already experienced a cyberattack and may not even know it since attackers can penetrate a company's walls and **remain undetected** for over 200 days.

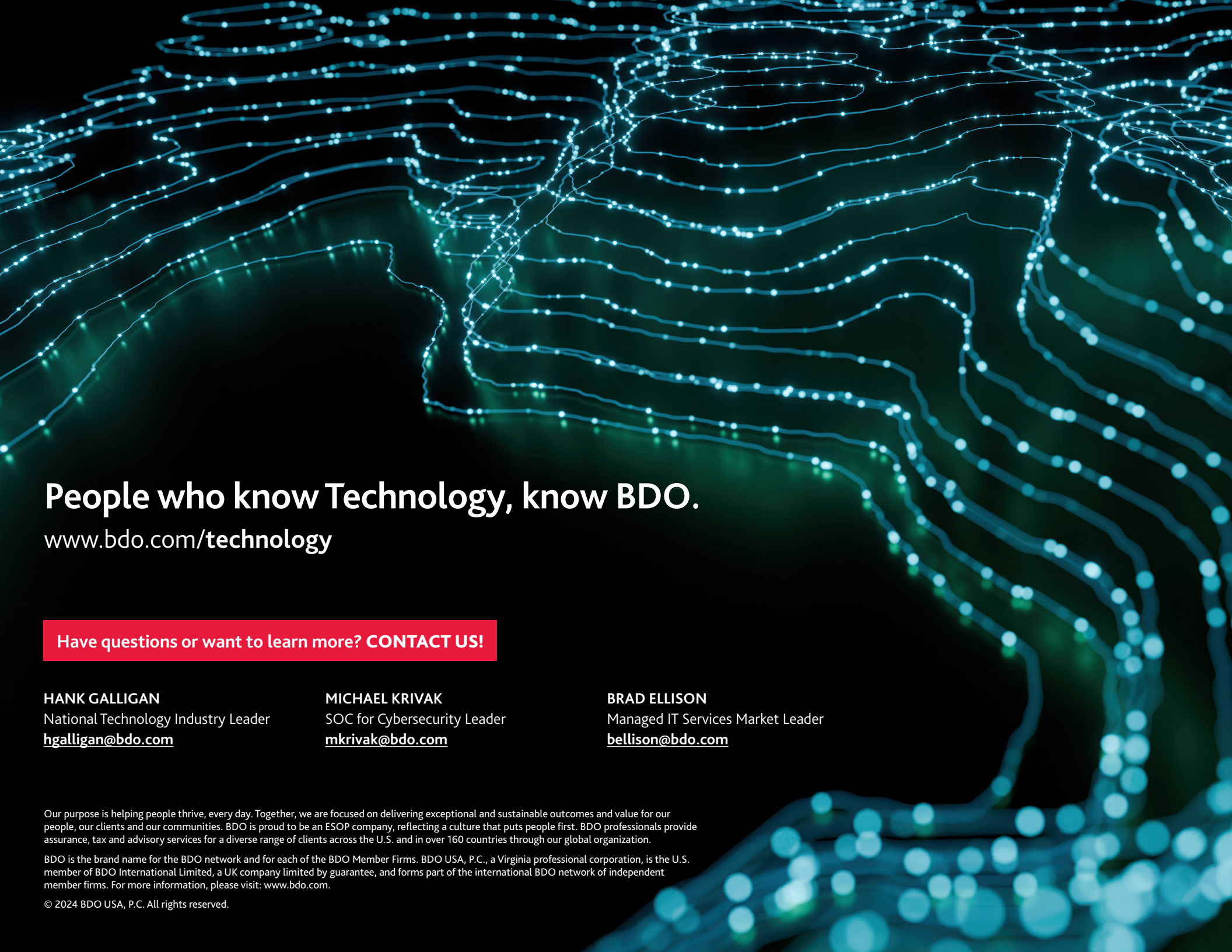
How BDO Can Help

While the cyber threat landscape can be difficult to navigate amid heightened and more powerful attacks, a third-party advisor can help technology companies improve their defenses and build resiliency.

BDO can provide co-sourcing for tech companies who do not have the IT budget, capabilities, or resources to independently address cybersecurity gaps, mitigate cyber risks, or prepare for regulatory reporting. In a co-sourced model, internal IT teams work with BDO professionals to develop or enhance security practices that protect the organization's confidential data.

In addition, BDO's **third-party attestation** professionals can conduct a gap analysis to help tech companies identify and address issues with their cybersecurity practices. From there, BDO can compile a thorough System and Organization Controls (SOC) for Cybersecurity report that companies can use to communicate their cybersecurity posture to key stakeholders.

To learn more about how you can navigate the evolving cyberthreat landscape, read our 2024 State of Cyber Report ▶



People who know Technology, know BDO.

www.bdo.com/**technology**

Have questions or want to learn more? CONTACT US!

HANK GALLIGAN
National Technology Industry Leader
hgalligan@bdo.com

MICHAEL KRIVAK
SOC for Cybersecurity Leader
mkrivak@bdo.com

BRAD ELLISON
Managed IT Services Market Leader
bellison@bdo.com

Our purpose is helping people thrive, every day. Together, we are focused on delivering exceptional and sustainable outcomes and value for our people, our clients and our communities. BDO is proud to be an ESOP company, reflecting a culture that puts people first. BDO professionals provide assurance, tax and advisory services for a diverse range of clients across the U.S. and in over 160 countries through our global organization.

BDO is the brand name for the BDO network and for each of the BDO Member Firms. BDO USA, P.C., a Virginia professional corporation, is the U.S. member of BDO International Limited, a UK company limited by guarantee, and forms part of the international BDO network of independent member firms. For more information, please visit: www.bdo.com.