Voice of the CIO

How are CIOs balancing risk, trust, and opportunity

In an ever-evolving business environment, chief information officers (CIOs) face numerous interrelated challenges.

A new wave of cybersecurity risks, fueled by geopolitical tensions and powered by artificial intelligence (AI), has materialized. Unsurprisingly, the threat landscape continues to evolve as criminals—both organized and state-backed—seek new opportunities to create chaos and extract profit from a rapidly evolving digital environment and the information that flows within it.

We encourage organizational leaders, particularly CIOs, to whom security and technology teams often report, to acknowledge that they're never going to be able to protect against everything. Organizations are always going to carry some degree of cyber risk and despite all due diligence, security controls can, and often do, fail. If companies try to protect against every risk, not only can the budget demand become burdensome, but also the opportunity cost can be onerous given the impact of security measures on operations and business activities.

We believe that moving forward in a modern, digital environment demands an evolved focus on cyber resilience, such that the ability to quickly detect, respond to, and resolve cyber incidents becomes a business-as-usual activity.

In the latest installment of our ongoing series of conversations with CIOs, we convened a distinguished group representing a diverse cross section of industries to discuss the state of cybersecurity and how they are working to mitigate the impact of cyber incidents and protect their organizations. Through this discussion, several priorities emerged: the concept of zero trust; the Securities and Exchange Commission's (SEC) recently adopted cybersecurity rules; third-party risk; and the opportunities, and challenges, around AI and automation.

Zero trust on the front burner

As 2024 kicks off, the threat landscape continues to evolve and bad actors are getting better.

Companies across the industrial spectrum are working to mature the cybersecurity model and change the paradigm from acquiring more and more tools to focusing on zero trust—a strategy under which no user, human or machine should be trusted by default and must be reauthenticated continuously.

The question becomes: Are companies just building a stronger "castle and moat" versus pushing the envelope and changing their approach?

To the CIO of an automotive equipment supplier, it seems like a never-ending quest for new tools that are only a slight improvement over something else.

"As a manufacturing organization, we have a heavy presence in the OT environment, which creates its own set of risks relative to IT," they said. "We're looking into network segmentation, but zero trust is the major discussion for us."

One CIO said they are trying to prevent that initial penetration and increase the speed at which they respond, but conceded that, in many ways, the existing model is fundamentally broken.

And so, we're looking at redeploying investments into zero trust and thinking about segmentation further.

Across industries, one of the biggest challenges CIOs and their teams are facing is keeping business priorities top of mind. Managing the disruption that a transition to a zero-trust approach can create is a clear challenge simply because it takes longer to deliver a product or service when users only have access to specific resources through the principle of least privilege.

Implementing zero trust across the various layers of cybersecurity requires a business conversation, but many nonsecurity team members are not actively immersed in the nuts and bolts of the process. It's clearly a learning journey for the entire business.

What has helped, according to the CIO of a major consumer products company, is getting buy-in at the top of the house, from the C-suite and the board, in terms of transitioning to zero trust.

The consensus among the CIOs is boards are more tech and cyber savvy than ever. Cybersecurity, in particular, has become a top priority at the board level, as well as among senior leadership, and that awareness is starting to trickle down through the organization.

Many CIOs, or their chief information security officers (CISOs), do a cyber review during audit committee meetings. "There are still lingering questions from the business around why IT makes things difficult or acts as a speedbump, but we're getting much less pushback on budget requests and policy changes than we've seen in the past," said the consumer products CIO.

They know it's a matter of "when," not "if," an incident will happen.

Purely from a cybersecurity perspective, CIOs largely agree that consolidation must occur in the market. The never-ending stream of products that companies feel the need to plug in and activate to keep their environments secure is just not sustainable as a practical matter.

To that end, it appears the ongoing shift in cybersecurity toward platform players—the primary cloud hyperscalers in particular—is primed to accelerate. Indeed, the investments big tech companies are making around embedding cybersecurity tools within their cloud platforms suggest that is the direction the market is going.

While some companies continue to study zero trust, others are executing. As the CIO of a women's clothing and beauty retailer highlighted, "We implemented zero trust and completely replaced our existing VPN approach. Initially, there was friction from employees due to the additional verification steps, but once they saw how simple it is, that they no longer have to dial into the VPN network every day, adoption went smoothly."

But it's not like flipping a switch. Across the board, the CIOs recognize need to promote ongoing education across the enterprise to help nonsecurity personnel get a handle on what these new processes mean to their day-to-day business lives.

In many cases, CIOs and their security teams are feeling the pressure from all sides—the board, the business, and operations. Some of the recent, high-profile cyber incidents have affected board and senior management thinking about security and privacy. CIOs know it's critical to keep driving knowledge and awareness through real-world training.

One participant, who is a CIO at a leading pharmaceutical company, said, "We've learned to educate our board and business leads. It's still a journey, but we have started to change the language from, "slowing down to increase security", to, "unlocking value while maintaining security.'"

"One of the things we realized," the CIO continued, "is the folks who are in relationship roles within the business are too often not aligned with the application architects. So, we've focused on increasing cyber awareness and embedding security processes within our application development teams."

Some may call it DevSecOps, which has in many cases become about tooling, but the objective is getting that mindset more deeply embedded into the teams who are making the development decisions at the application level.

"Security is just as important as quality for us, but it has been an iterative process," said the pharmaceutical CIO. "We're trying to codify the model so we scale it. I won't say we have it nailed, but we are certainly starting to understand that zero trust is going to be a value accelerator for us."

It's about security teams aligning with the board and C-suite on an acceptable risk tolerance level. That enables organizations to understand the level of technology investment that makes sense to keep the network secure.

Actions to consider now

- Accept that adopting a zero-trust approach isn't a project, it's a journey—it takes time to implement.
- Get all stakeholders engaged early in the transition process.
- Establish a roadmap with specific, realistic milestones that align with business priorities, emerging threats, and budgets.

Making sense of the new SEC cybersecurity rules

In July 2023, the SEC introduced new rules requiring public companies to disclose within four days cybersecurity incidents they deem material[1]. The big question for CIOs and their teams has been how organizations are determining materiality when an incident takes place.

The rules greatly expand the cybersecurity disclosure obligations to which organizations must adhere. It's a significant undertaking and board oversight is essential.

In many cases, the preparation of these cybersecurity disclosures will require a reassessment, and perhaps modification, of the company's existing risk management processes. Most companies have general thoughts about these requirements, but materiality likely is going be handled on a case-by-case basis.

It's worth noting that the language in the SEC guidance measures materiality against how a reasonable investor would consider the incident's impact. Nebulous and open to interpretation as that language is, CIOs saw the challenge right away.

The CIOs we spoke with acknowledge they don't have all the answers and expect to rely heavily on their general counsels to ensure proper compliance.

There's an ongoing learning curve across the organization to determine what is material and there is concern over making disclosures within the four-day timeframe if the incident is impacted by a law enforcement delay or national security implications.

An example one CIO offered was business email compromise. "If a CEO's email account is hacked, then that likely would immediately be viewed as material," they said. "But if an engineer's or administrative assistant's email was impacted, it might not be. Clearly, there's a lot of room for interpretation. The SEC's guidance has led organizations to err on the side of disclosure, but it can be a slippery slope."

Most organizations don't seem to have done anything to alter the committees that evaluate the need for disclosure or determine materiality, but the common refrain is for constant communication with the board and doing a broad IT update once

[1]Source: U.S. Securities and Exchange Commission, "SEC Adopts Rule on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies" (July 26, 2023).

or twice a year, inclusive of both internal external cyber issues and trends.

A CIO of a large transportation services company cited the value of the personal approach. "We put together a quarterly one-page report for the board and the audit committee that features fairly granular security metrics and relevant news."

Actions to consider now

- Establish a good relationship with your general counsel and talk early and often with them about the new SEC cyber rules.
- Create a committee to define the organization's view on what constitutes a material incident; reassess that definition at least quarterly.
- When discussing materiality, consult with your insurers to determine exposure from that perspective.

Third-party risk, first-order priority

According to the CIOs in this session, a significant number of cyber incidents documented over the last year or so were related to the vast ecosystem of third-party providers, from suppliers and vendors to distributors and resellers.

And these events were not necessarily data exfiltration. One CIO related a scenario in which a third-party logistics provider was hacked and a delivery address was changed so contents of a truck were stolen. "Our cybersecurity team spends a lot of time documenting cases like that with all the right parties involved to make sure we understand business impact, all the legal issues, if insurance was involved, etc.," the CIO said. "All that information is packaged and communicated up to the board."

Virtually all CIOs cited strong cyber review processes at their company for monitoring and identifying organizational risk exposure across the entire partner ecosystem. However, with thousands of outside vendors they simply cannot review all third parties individually.

"There's no way we can ever have a one-size-fits-all approach to third-party security," said the CIO of an international automotive manufacturer. "But it is critical to develop a level of comfort regarding the internal security of the third parties with whom you work."

Companies realize they must look to prioritize security within any third party that might be able touch, handle, or otherwise utilize customer or enterprise data.

To that end, they've identified their top 50 global suppliers who, if they were impacted by a cyber event, could cause one of the company's manufacturing facilities to shut down. "Beyond existing contractual obligations, we are now going to those suppliers and performing annual audits of their processes to ensure they are as secure as possible. We're going above and beyond just reinforcing contracts."

This is particularly important for some of the smaller tier 2 and tier 3 suppliers that don't have the technological or financial capabilities to perform regular security assessments and upgrades.

"We view this shifting left of security to be vital because we need our suppliers and vendors to be better, so we can be better," the CIO said. "We can't afford to have one of our large factories go dark, even for a day or two, because one supplier can't perform basic services."

As for logistics providers that facilitate container ship and rail deliveries, some of the larger organizations are looking at insourcing those processes so they control more of those processes directly.

Another CIO pointed to the supply chain side of the third-party universe, where they're not only scrutinizing contractual terms, but they're also bringing in another vendor to perform audits. "We're doing these framework-based audits and adding contractual provisions that stipulate if they can't demonstrate an acceptable level of security, we're going to discontinue working with them."

Companies cannot bury their heads in the sand and ignore third-party risk. The vast ecosystem of suppliers is what propels business in today's global economy.

The CIO of a healthcare services provider cited their strategy around maintaining multiple partners to enable the company to have contingency plans that involve fourth-, and fifth-party partners should they experience an incident. "We need those backups because we're so wired to get the best partner, the best deal, that we often lose sight of what could happen if our primary vendor is compromised. Suddenly, we could have a contractual problem or, worse, a regulatory issue because the supplier is down for a week and we can't meet our obligations."

Actions to consider now

- Decide whether it is in the best interest of the organization to move on from less-sophisticated suppliers who cannot confirm the necessary level of technological or security maturity.
- Enhance transparency to build trust across suppliers and vendors.
- Rather than treating third-, fourth-, and even fifth-party relationships solely as transactional and contractual, approach them as an extension of your ecosystem.

AI and automation: Opportunities and challenges

A dynamic topic that cuts across all others is the influence on cybersecurity of automation and AI and how these ever-evolving cognitive technologies are altering the thinking of CIOs and their teams.

From a third-party perspective, the discussion focused on getting away from spreadsheets and investing in platforms and AI to gauge third-party risk. "We use a platform for our third-party cyber reviews," said a consumer products CIO. "We used to do it with spreadsheets and long lists of questions—it was just untenable."

The more CIOs are going to have to be accountable for monitoring suppliers and reporting on incidents—clearly, these activities are time consuming under the best of conditions—the more interesting and valuable automation and AI has become.

It's daunting enough just staying on top of the various threat vectors and remaining compliant, said the CIO of a leading multinational food company. "We are exploring all possible strategies for getting ahead of these responsibilities and automation and AI are at the top the list."

It's interesting to note that, despite the acknowledgment of the promise of AI, at this point, AI is something this and other CIOs are still exploring and studying. They have not fully jumped into activating it, broadly speaking.

Pivoting to GenAI, the CIO of a leading supplier of building materials highlighted the discussion in the industry around developing new capabilities within a protected GenAI "sandbox" focusing on specific business use cases. Harvard University describes the sandbox as providing "a 'walled-off,' secure environment in which to experiment with generative AI, mitigating many security and privacy risks and ensuring the data entered will not be used to train any public AI tools." [2]

But, of course, GenAI poses unique risks and many organizations are adjusting existing security practices in response. According to the food company CIO, "Our thought was let's at least have some basic ground rules. We saw people across the organization getting very curious about GenAI—and rightly so. We wanted to ensure people are training the algorithm appropriately, prompting it effectively, and using the output responsibly and securely. Otherwise, we feared GenAI becoming the digital equivalent of the Wild, Wild West."

They partnered with legal to establish a clear, formal policy. Viewing it as a base-level minimum, we shared the document with the full organization, saying these are your GenAI guardrails.

The women's clothing CIO spoke of a monitoring tool that goes into the cloud platform and standing up an AI Council that stays on top of the data that goes in and out. This CIO oversees the budget for all AI activity enterprise-wide and reviews all AI-related requests and the related business case and must sign off before it goes forward.

Reflecting the broad market's reticence, a number of CIOs reported restricting access to OpenAI's ChatGPT soon after it launched and putting a governance process with an exception policy in place. Employees at some of these companies still must attest to the policy and demonstrate a legitimate business need before they can access the tool.

A healthcare company's CIO highlighted an enterprise program into which all of their GenAI use cases are funneled. As new partners and vendors present new AI opportunities, the organization will have to step up its monitoring to avoid data leakage through third parties that have neither the same level of risk tolerance nor a mature governance model.

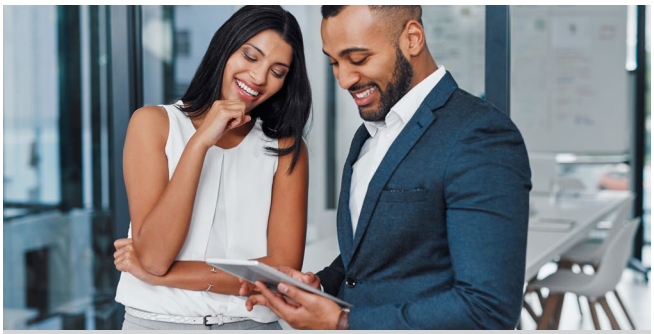
Another CIO acknowledged their organization, a building materials retailer company, is conservative and made the decision to shut down external GenAI tools. But knowing they had to keep up with the trend, they built an internal GenAI tool governed by a formal policy and now are piloting 100 business use cases. That enables them to manage in a more structured fashion to test whether the written policy is sufficient to deliver business value securely and within the risk tolerance level the organization is able to accept.

While there's clearly a need to go boldly, but not blindly when it comes to GenAI, it appears that some organizations will simply take their time while others will jump right into the deep end of the pool. Said one CIO, "I think we get too caught up in our own processes. Sometimes you need to just run it and manage the risk."

[2]Source: Harvard University Information Technology, "AI Sandbox pilot launches" (September 4, 2023).

Actions to consider now

- Augment existing skill sets to ensure broad AI awareness and understanding of the relevant data science through training, upskilling, reskilling, and bringing in new talent, as needed.
- Explore and avail yourself of cutting-edge AI-related tools available in the market to augment your ability to map, monitor, and attest to the security of your models.
- Consider developing an AI center of excellence to align organizational thinking on cybersecurity, privacy, and ethical AI.



Additional insights

The KPMG Trusted AI approach

SEC's Final Cybersecurity Rules: A Board Lens

Third-party security assessments

Navigating Zero Trust Security in the Remote Work Era

Connect with us

Marcus Murph
CIO Advisory Leader
KPMG LLP
214-280-8992
marcusmurph@kpmg.com

Steve Barlock
Cyber Security Services Cloud Leader
KPMG LLP
415-963-7025
sbarlock@kpmg.com

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

Learn about us: **kpmg.com**