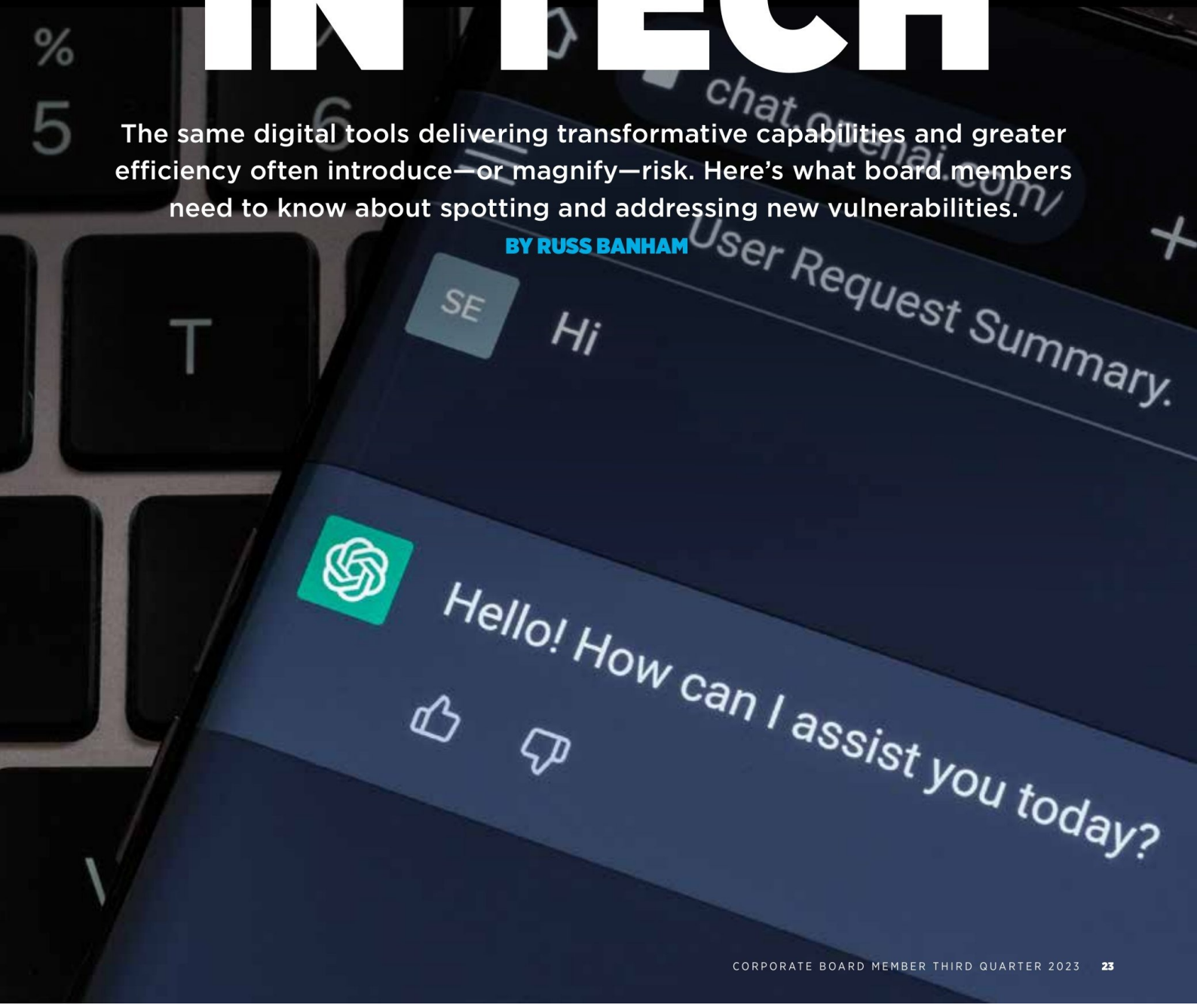
TRUSTING IN TECH

The same digital tools delivering transformative capabilities and greater efficiency often introduce—or magnify—risk. Here's what board members need to know about spotting and addressing new vulnerabilities.

BY RUSS BANHAM



Veteran board member Lisa Greer Quateman recently heard a harrowing tale that illustrates just how very wrong leaning into new tech tools can go. It began simply enough: The founder of a private equity fund decided to experiment with the generative AI chatbot ChatGPT. "He's Jewish and wanted the AI tool to create a fun story about a Jewish magic dragon for his kids," said Quateman, a board member at Western Asset Mortgage Capital, Scherzer International and Lyles Diversified. "The resulting story was full of antisemitic tropes. It was a horrifying example of why companies and board members can't place their trust in generative AI now, maybe ever, certainly not fully, he told me."

ChatGPT creator Sam Altman's recent testimony before Congress acknowledging his own fears underscored that sentiment for many. "My worst fears are that [the AI industry] will cause significant harm to the world," Altman said.

Despite such credible concerns, it's only a matter of time before generative AI, like so many digital technologies before it, is widely embraced by and adopted by businesses. And new digital solutions are hatched each day, pressuring companies to invest in these tools at their formative stages. Meanwhile, management teams and boards already struggle to foresee and head off potential issues stemming from the technological advances that have been transforming operations, especially the ongoing risk of a debilitating cyberattack.

In this complicated environment, board members struggle with four key concerns: Whether digital data, the feedstock of so many business decisions is pertinent and accurate; if the algorithms weighing different data-driven metrics are biased and create unjust outcomes; if a planned investment in an expensive new tech product is aligned with strategy and offers a measurable return; and if the cybersecurity framework and transfer of cyber risks to insurance markets will, in fact, withstand the business disruption caused by a major cyber incident.

For years, cybersecurity has ranked as the issue directors find most challenging to oversee and the one they are most concerned about confronting, according to *Corporate Board Member*'s 2023 What Directors Think survey, held in partnership with Diligent. What's more, two-thirds of directors participating in a 2023 survey by *Corporate Board Member* and RSM rated cyber risk a significant concern when it comes to digital transformation.

Yet, the RSM-*CBM* survey found only a small fraction of the digital transformation budget for 2023 has been allocated to strengthening cybersecurity (12 percent on average). In light of such worrisome findings, why aren't directors doing more to discern the true state of cybersecurity?

"Blind faith in what they're being told," replies Christopher Hetner, former senior cybersecurity advisor to the Securities and Exchange Commission. "On average, 70 percent of the board members still don't understand what's being delivered around cyber risk into the boardroom. The reports delivered by the chief information security officer are riddled with technical jargon and not contextualized to business, operational and financial risk."

How widespread is this mismatch? "I'm a former CISO at GE Capital, and I saw bogus metrics being brought to the board that were not reflective of our cyber risk exposure, not reflective of reality," says Hetner, the architect of the initial internal draft of the SEC's cybersecurity disclosure proposal under former Chair Jay Clayton. "The laser is pointed at the board. Are you really doing your job?"

"On average, 70 percent of board members still don't understand what's being delivered around cyber risk into the boardroom."

—Christopher Hetner, Former Senior Cybersecurity Advisor, SEC

TOUGH NUT TO CRACK

The severity of Hetner's comments underscores how crucial it has become for board members to challenge senior

My worst fears are that [the AI industry] will cause significant harm to the world."

—Sam Altman, CEO, OpenAI

management when told the organization's technology expenditures, data accuracy, algorithmic fairness and cyber risk protections are state-of-the-art, world-class and nothing to fret over. Not that this is a simple task to perform for otherwise broadly skilled directors.

"We as board members can't sit down and look at the code that has been written; we have to trust in the information that is presented to us and the quality of people in the organization providing it," says Susan Skerritt, a member of the board at publicly traded companies IG Group and Tanger Outlets. "Our job is to ask questions and listen carefully to the answers."

That job is becoming more demanding every day, adds Jeff Knauss, a board member at Community Bank System,

THEIR RISKS ARE YOUR RISKS

IT'S ONE THING FOR BOARDS TO OVERSEE management's activities to reduce the threat of a paralyzing cyberattack and quite another to ensure the company has vetted the cyber risks of its many partnering organizations. "A major ransomware attack may not hit your company, but if it infects the systems and disrupts the ongoing business of key suppliers, banks, cloud vendors or other partners, your business will feel the repercussions," says Timothy Zeilman, vice president at cyber insurance company HSB. "When they're down, you may be down, too."

He's referring to what the insurance industry calls a systemic risk event, a single cyberattack that spreads laterally to interrupt ongoing business activities at potentially thousands of companies. The good news is that such a major loss-producing event has yet to occur. The bad news is that one came so close that major cyber insurers like Lloyd's of London and others have tightened policy language and added coverage exclusions reducing their exposure.

The cyber incident that came within a hair of causing such a domino effect was the launch in 2020 of a so-called "supply chain attack," a type of cyberattack aimed at the weaker links in a company's supply chain. The attack involved 18,000 customers of software company SolarWinds receiving a software update compromised with malware, subsequently named Solarigate.

The customers included tech giants Microsoft, Intel and Cisco and multiple U.S. government entities, such as the State Department and the Pentagon. Fortunately, the data of only nine federal agencies and about 100 private-sector companies was compromised. The organizations were advised to take their systems offline and undertake costly decontamination processes. If the number of infected entities had been in the tens of thousands, potentially hundreds of thousands of companies that relied on the services of the compromised organizations could have experienced a disruption in ongoing business.

Other cyberattacks also came close to unleashing a systemic event. In 2021, a cyberattack called a Zero Day Exploit was launched to discover an unknown vulnerability in a widely used software product. The product in the crosshairs was Log4j, an open source logging utility embedded in hundreds of millions of computers. The following month, Microsoft's Defender Threat Intelligence unit picked up the threat, and U.S. government cybersecurity officials subsequently issued an emergency directive requiring all federal agencies to patch the vulnerability.

Had the hackers succeeded, millions of entities that used Log4j could have been prevented from accessing the data in their systems, disrupting ongoing business. "Many CISOs do a great job preventing and monitoring their organization's cyber incidents, but when it comes to a systemic event, boards need to consider calling in the company's director of risk management, heads of compliance and legal, and senior executives for their perspectives," said Zeilman.

The risk manager is an important resource to ensure adequate insurance protection at a time when major cyber insurers are adopting exclusions involving state-backed cyberattacks, with some creating separate, higher-cost insurance policies for systemic risks.

"Board members need to ask questions and challenge senior management on such concentration risks," said Wes Bricker, vice chair at PwC. "In these risk assessments, management should be asked for the scenarios that could cause a system risk and what will be done in this event to ensure timely data information flow from connecting organizations. This is all about resilience." *—RB*

DISCLOSURE DILEMMAS

Yet to be finalized, the long-awaited rules proposed by the SEC would require publicly traded companies to disclose material cyber incidents within four days along with their cyber risk management, strategy and governance. The proposed rules include a mandate—that management disclose directors' cybersecurity expertise—causing consternation in boardrooms.

For one thing, management would be required to disclose in their annual reports or proxy disclosures the board of directors' cybersecurity expertise. They would also have to disclose the processes used to communicate cybersecurity risks to the board and the frequency of those discussions. Most board members have only basic knowledge of cyber risks, and many feel this level of expertise should be enough.

The disclosures detailed in the 129-page Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure proposed rule are meant to protect investors, according to SEC Chair Gary Gensler. In a statement announcing its release, Gensler called cybersecurity an "emerging risk" and said the proposed rules would ensure that cyber risks are reported in a "consistent, comparable and decision-useful manner (for investors)."

Many public comments following the release of the proposal pertained to the difficulties in determining a cyber incident's materiality within four business days of its discovery. As PwC wrote, "completing a materiality determination could take several weeks to months from initial identification of an incident, depending on its complexity." The audit and advisory firm stated that it supported disclosing a material cyber incident "as soon as reasonably practicable," as opposed to four business days.

"Cyber is a bit tough to course out when it comes to materiality," Justin Greis, partner and leader of McKinsey's cybersecurity, digital and technology practices, commented in *Corporate Board Member*'s sister publication StrategicCFO360.com. "If a hacker gains access to a company's customer list and puts it on the Dark Web, that's clearly a material impact. On the other hand, say there is evidence that a hacker has gained access to the network and is doing network reconnaissance and enumeration but hasn't actually exfiltrated any data. That's important information to the company, but whether it's material for reporting purposes isn't clearly defined. It's a question mark."

Another area cited as problematic involves the disclosure of the procedures used to identify and manage cybersecurity risks. The challenge in providing this information is how much to provide. If registrants under-report their cybersecurity risks and suffer a major cyberattack, this could be ammunition for a successful plaintiff lawsuit. If companies over-report their risks, they could expose a potential cybersecurity weakness.

Obviously, boards have their work cut out for them, as does management. Small wonder the SEC has yet to issue a final rule: Many comments on the proposed rule explicitly request a delay in implementation to iron out the kinks. According to the Office of Management and Budget, the final rules were expected as early as April 2023. The wait

"No board member can keep up with the ever-evolving AI tools that come out."

—Jeff Knauss, Board Member, Community Bank System, United Way, CenterState CEO and SUNY Oswego

United Way, CenterState CEO and SUNY Oswego. "No board member can keep up with the ever-evolving AI tools that come out," he said. "Just two weeks ago, I read that 200 AI tools were released in one week, many of them by brand-new companies."

Susan Mallory, a board member at Occidental College in Los Angeles, cites an alarming report that she and other board members recently reviewed. "In November and December of last year, after ChatGPT was released, plagiarism went up one million percent," said Mallory, who also serves on the boards at Scherzer International, AI startup Wealthawk, and other companies. "Educators are aghast and are trying to put governance around this."

Governance is crucial, agrees Mark Weinberger, board member at publicly traded companies MetLife, Johnson & Johnson and Aramco. "What is important for directors is to ensure that the opportunities and risks inherent in any new technology, whether it involves AI, automation, data privacy or cybersecurity, are assessed and managed through a governance framework," Weinberger said.

"There is no digital strategy or IT transformation strategy," he asserts. "There is only a business strategy. The

Whenever a cool new AI investment is introduced by management, a big warning light should go off for directors."

—Steven Horowitz, Board Member, SCWorx and Careviso

board's duty is to make sure that the investment will further the strategy—which requires that they understand the technology in the first place. That often means getting third-party input around the right questions to ask in order to gauge the potential risks."

But what if the answers are incomprehensible? "Typically, in my experience, when the CIO or CISO are asked difficult questions by the board, they default to 'tech talk,'" says Hetner. "I've had candid conversations with Fortune 500 CISOs who told me they've trained the board to be compliant, even after a material data breach."

A survey by Cybersecurity at MIT Sloan (CAMS), a research consortium, and enterprise security company Proofpoint, appeared to lend credence to this view, stating that 65 percent of board members think their organization is at risk of a material cyberattack, but only 48 percent of CISOs share that view. Only 47 percent of boards regularly interact with the CISO, with less than a third of board members seeing the CISO only during board presentations. "Directors and security leaders spend far from enough time together to have a meaningful dialogue about cybersecurity priorities and strategies," the researchers wrote in *Harvard Business Review*.

Yet, cybersecurity is often cited as a top board concern, as was the case in a recent survey of 164 board audit committee members by Deloitte's Center for Board Effectiveness and the Center for Audit Quality (CAQ). Knauss says these concerns will increase as hackers begin to deploy AI tools in their arsenal. "AI can be used to get smarter around things like password breaking and circumventing firewalls and passwords," he says. "Think about how easy AI is going to make a phishing attack. Using ChatGPT or other generative AI natural language tools, they can make them sound exactly like the person they're pretending to be. Everything becomes more convincing and increasingly smarter due to machine learning in the AI."

Board members are painfully aware of the uphill climb before them. "As much as we rely on highly qualified managers, the company can't be as bulletproof or as safe as we hope," says Quateman. "Good board members need to bring a healthy dose of skepticism about the organization's cyber preparedness to the boardroom."

Adequate skepticism also needs to be applied to a company's expenditures on technology. "I've seen management time and again go to the board with plans to overspend tens of millions on tech and cybersecurity, and instead of the board asking management to provide the strategic value for the spend, they rubber stamp it," Hetner says.

Skerritt agrees. "Every company has different technology needs, which is the case with the two public company boards I'm on," she says. "At IG Group, a derivative trading platform headquartered in the UK, technology is fundamental to them—as they're a fintech; it's their most important product set. Alternatively, at Tanger Outlets, their primary business is providing space to retailers to sell [products] in an outlet. The strategic relevance of technology and the value it delivers is less important, as it's not their primary focus."

The more difficult challenge is when senior management argues a competitive need to invest in a new technology driving perceived improvements in productivity and efficiency, the case with many AI solutions and tools. "Is the organization throwing money at the latest AI fad, or is it central to strategy?" questions Steven Horowitz, board member at private and public companies such as SCWorx and Careviso. "If it is central to strategy, how does the algorithm work? How can we be sure it isn't skewed one way or another or won't produce false positives? Whenever a cool new AI investment is introduced by management, a big warning light should go off for directors."

The warning light should be blinking with generative AI, a term describing an algorithm that produces an outcome based on data it has been trained to collect, collate and interpret. Such AI models are touted for their "decision support," the rapid presentment of information to business leaders to make more insightful decisions. This prospect in part is expected to catapult the global generative AI business market from $1.2 billion in 2022 to $20.9 billion by 2032, a 33 percent compound annual growth rate, according to a recent market analysis.

There is no digital strategy or IT transformational strategy. There is only a business strategy."

—Mark Weinberger, Board Member, MetLife, Johnson & Johnson and Aramco

But what if the underlying data used by the algorithms to model the conclusions is inaccurate, dated or biased? "As with every new technology, business leaders must proceed with eyes wide open, because the technology today presents many ethical and practical challenges," McKinsey & Co. cautioned in a recent report on Generative AI.

Board members should exercise similar circumspection. "I'd be wary if management comes into the board meeting with huge investment plans in generative AI, which is pretty early stage," says Horowitz.

Knauss advises similar caution, but not to the point of potentially tossing out the baby with the bathwater. "AI tools are not 100 percent accurate, far from it, but they can provide a head start in providing more efficient ways to process information," he says. "The board needs to challenge management teams that seem super eager to use tools that are untested and dangerous, but also those that appear slow to react to the opportunities of AI."

DISCLOSURE DYNAMICS

Several board members commented on the impending SEC cyber risk disclosures and reporting rules. In the proposal floated by the SEC for review last year, companies would have to disclose their cyber risk strategy, governance and practices, and the specific role of the board in these regards. According to the Deloitte and CAQ survey, the majority of respondents (53 percent) delegate cybersecurity oversight to their audit committees.

"The audit committee is ultimately responsible to evaluate regulatory disclosures and controls," says Quateman. "An argument can be made that the committee needs additional resources to address the inherent complexities (of the SEC cyber risk disclosures)."

While the Deloitte/CAQ survey indicates that audit committees are looking to increase the number of board members on them, should these new members be professional AI and cybersecurity experts equipped to hold management's feet to the fire? Hetner demurs. "Shoving cyber experts on the board is not a solution," he says, "as they don't understand the business and operational context to offer helpful guidance on the costs related to cybersecurity. Ask them about things like debt financing and they're blank faces."

Weinberger says that directors on the boards on which he serves benefit from the use of the public companies' enterprise resource management dashboards, which they can access to review the risks related to technology prior to board meetings. "We look at the dashboards on a regular basis to assess how management is responding to various technology and cyber risks. We also have external parties come in every year to evaluate what we're looking at. This is not a one-off discussion with the CISO; it's part of the overall risk framework."

TRUST AND VERIFY

There is no easy solution to the dilemma before boards. Given the likelihood that many board members will have a layman's knowledge of complex data, AI and cybersecurity subjects, the only ammunition they have is to firm up the toughness of the questions they ask senior management.

Every board member has a fiduciary responsibility to shareholders to say to the CISO or CTO, 'I need clarification around what you're saying.'"

—Jeff Knauss, Board Member, Community Bank System, United Way, CenterStateCEO and SUNY Oswego

Skerritt says that boards should train members in questioning strategies and techniques, starting with open and general questions, for example, and then drilling down into specific points. "There are different types of questioning processes members can use to gather information; the point is to pick one and effectively train the directors in these techniques," she says.

Skerritt adds that both internal and external technology and cybersecurity experts that come to board meetings should be told right off the bat to express their comments in ways that are understandable to people who don't have deep technical proficiency.

Knauss agrees. "Every board member has a fiduciary responsibility to shareholders to say to the CISO or CTO, 'Look, you either need to slow down or I need clarification around what you're saying, as you're spouting this alphabet soup of abbreviations and acronyms,'" he says.

Wes Bricker, vice chair at PwC, offers a similar perspective. "Board members have a duty of care and a duty of loyalty; they need a duty of challenge, to apply their curiosity and skepticism in challenging senior management when told this is what we're spending (on technology), what we're using AI models and algorithms for, and how we're managing our cyber risks," says Bricker, who co-leads the audit and advisory firm's U.S. Trust Solutions platform.

Bricker counsels the wisdom of having the CFO in attendance in board meetings with IT and cybersecurity leaders. "There's a classic, constructive tension between the CFO and the CTO around technology and cyber investments and their returns and outcomes," he says. "The CFO is positioned to ask what the business outcomes are, when they will be realized, and whether it is better to lead or lag when a tech innovation is introduced."

Other than ask ever-more-probing questions fueled by suspicion and doubt, what else can board members do to ensure management is telling the truth? Hetner says they should support regulatory aims to increase cyber risk transparency.

"Frankly, this is the purpose behind the SEC disclosures; in drafting them, we wanted board members, given their fiduciary duties to shareholders, to have more transparency around the financial and operational impact of cyber risks, by requiring companies to disclose material cyber incidents in four days and what they're doing to prevent and mitigate such incidents," he says.

"Our goal was and is to build a governance path forward," Hetner adds. "Only radical transparency can do that. We wanted boards to appreciate the immensity of the risk; only then could they effectively exercise their fiduciary responsibility to provide oversight guidance to management. The boards that get this have been extremely receptive."

Radical transparency would also give board members leeway to be more trustful of senior management in the performance of their fiduciary duties. Through the disclosures they would be able to effectively oversee management's preparedness to intercept a cyber incident, avert much of the business impact and transfer what remains to cyber insurers.

"Board members already have the basics; they just need to be a bit more courageous in asking questions," says Bricker. "If you don't understand or like the answers, rephrase the questions until you get what you want. You don't need to be an expert in generative AI or cybersecurity; that's what the inside and outside technical people are for. Your job is to ask the questions." **CBM**

Russ Banham is a Pulitzer-nominated financial journalist and best-selling author.