TAG

Security Annual

4TH QUARTER 2023

CYBER AND THE BOARD

ARTICLES / OPINIONS / INTERVIEWS

TAKEAWAYS FROM OUR BOARD BOOK

DAVID HECHLER, EDITOR

The feature articles in this issue, with one exception, are from *Guiding Cybersecurity from the Boardroom,* the book that we published on October 25 (see p. 4 for free download). The six we picked all offer lessons that should be helpful to corporate directors, but just as useful to others with an interest in, or a hankering to learn about, cybersecurity. The same could be said about the eight we did not include here. We chose these because they can be read quickly, and they cover a broad range of topics. And like the ones in the rest of the book, they were all written by individuals with deep knowledge and experience in this field. You'll be able to tell that didn't come from watching a video on YouTube. (We added the seventh article in order to include an outsider's perspective by interviewing someone who has not worked directly in this field but knows it well.)

Perhaps the best way to introduce this section is to preview some of the articles' takeaways. Reviewing them in order:

Melanie Ensign tackled crisis communications. Building credibility with the media before a cyber incident, she advised, can pay big dividends when one happens.

Dr. Edward Amoroso wrote about artificial intelligence. If a company's M&A due diligence doesn't include AI, he wrote, the firm runs the risk of buying an investment that AI is poised to replace.

Anne Chow discussed partnerships between management and boards. It's a misconception, she said, to think of cybersecurity as a technology issue. First and foremost it's a business issue.

Andy Geisse recounted his experiences with cybersecurity as a CEO and later as a board member. As important as it is to track security issues, Geisse wrote, it's also important to track efforts to prevent security issues.

John J. Masserini talked about identity management. It doesn't only keep your company safe, he noted. Potential clients are more likely to trust you.

Debora A. Plunkett explored a board's fiduciary responsibilities. Board members don't have to be experts in cybersecurity, she said, but they do have to know enough to ask the right questions.

Kyle McIntyre answered questions about his executive recruiting company that specializes in cybersecurity. You can hire an uppercase CISO or a lowercase ciso, he said. Just be sure you're clear about what you want and pay them accordingly.

"We have about three minutes before lunch. That should be enough time for our annual cybersecurity update."

TAG Cyber Security Annual
4TH QUARTER 2023

Lester Goodman, Director of Content

David Hechler, Editor

Contibutors

Dr, Edward Amoroso
Anne Chow
Melanie Ensign
Andy Geisse
Moriah Hara
David Hechler
John J. Masserini
David Neuman
Debora A. Plunkett
Joe Sullivan
Christopher R. Wilder

Editorial & Creative

Lester Goodman
David Hechler
Jaimie Kanwar
Miles McDonald
Rich Powell

Research & Development

Matt Amoroso
Shawn Hopkins

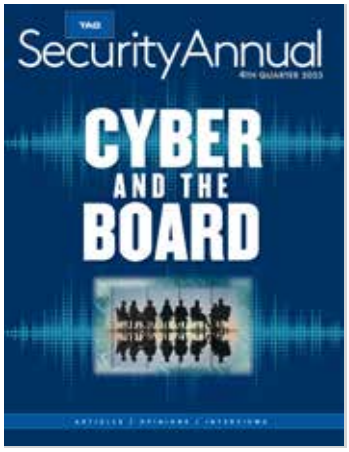
Sales & Customer Relations

Rick Friedel
Michael McKenna
Laurie Mushinsky
Julia Almazova
Jane Mangiamele

Administration

Liam Baglivo

Dr. Edward Amoroso, Founder & CEO

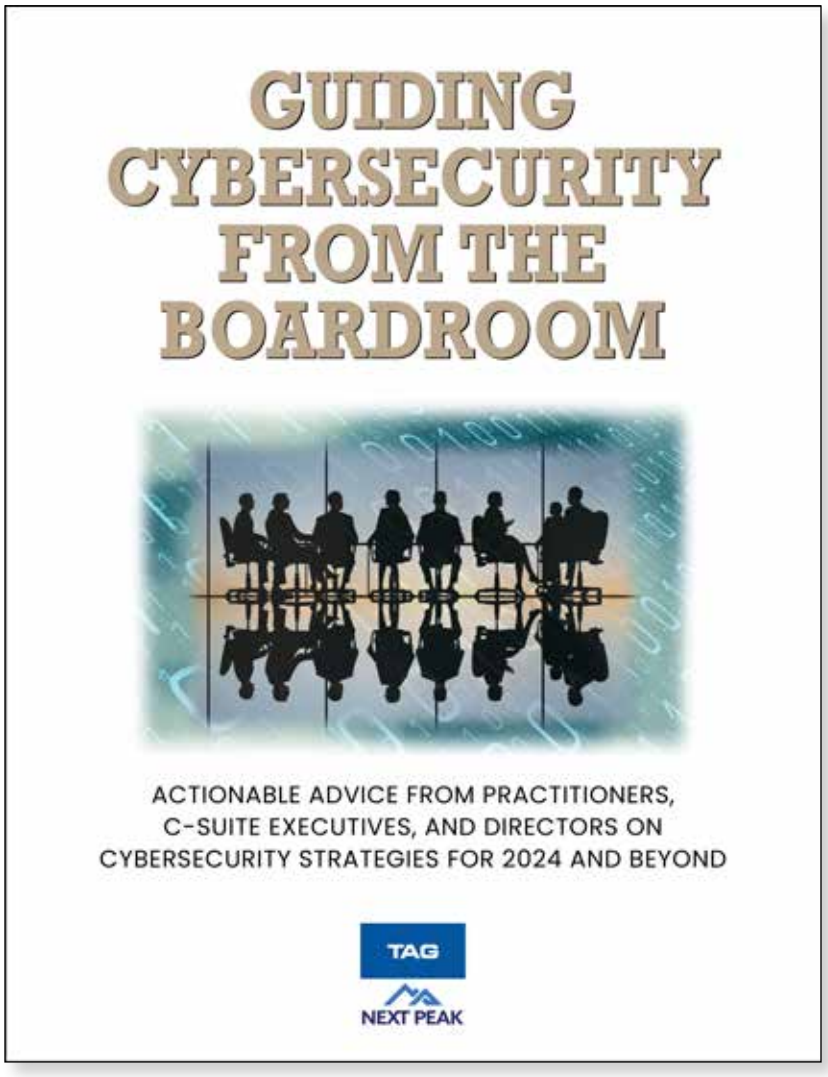


Volume 9 No. 4

Publisher: TAG, a division of TAG Infosphere, Inc.,
45 Broadway, Suite 1250, New York, NY 10006.

November 1, 2023

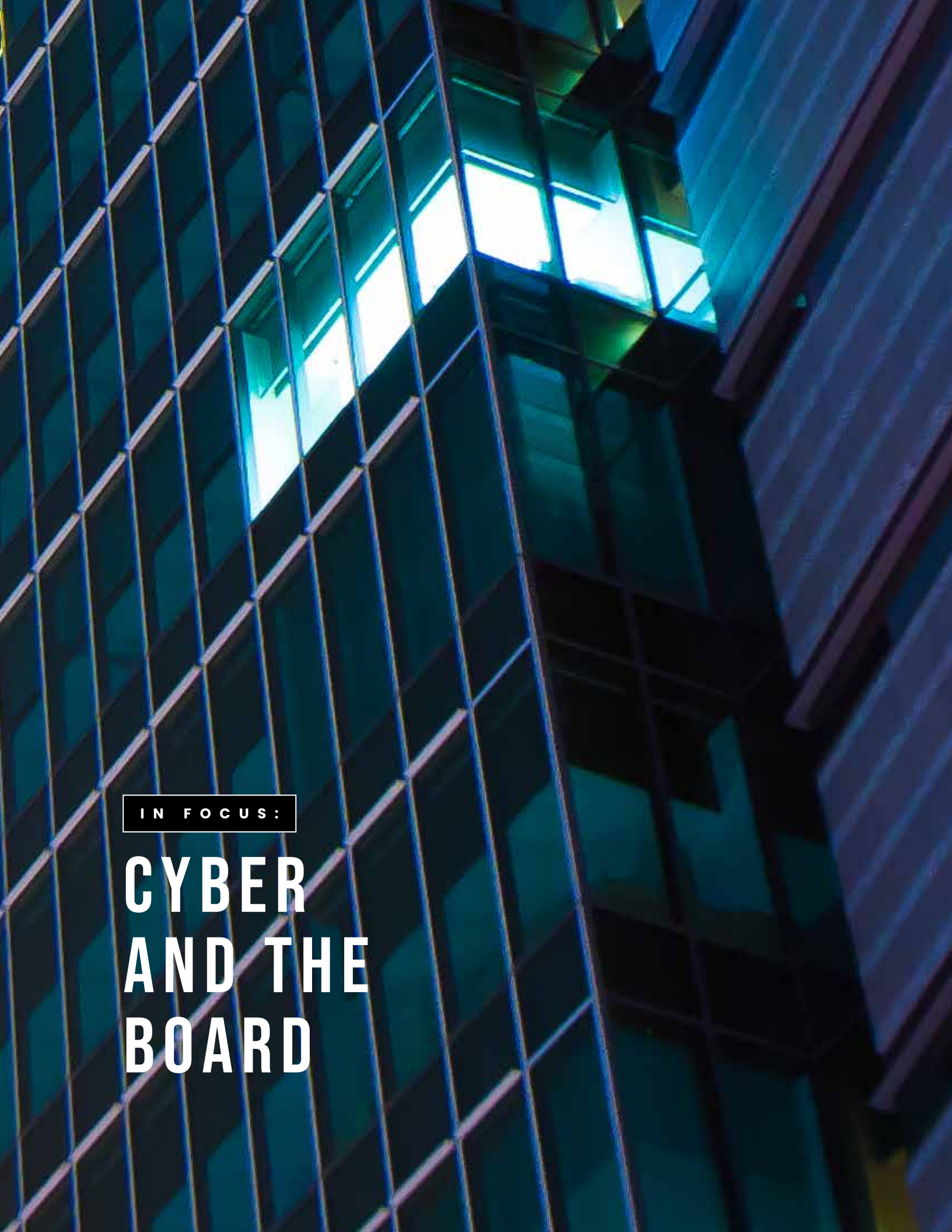
OUR NEW BOOK IS NOW AVAILABLE



A dozen cybersecurity practitioners wrote 14 chapters that cover a lot of ground. Crisis communications. Management-board partnerships. Artificial intelligence and quantum computing. In-house lawyers v. SEC regulations. Eventually each chapter circles back to boards of directors: what they know about cybersecurity, what they don't, and what they need to know.

The authors are and have been CEOs, analysts, professors, board members, CISOs, founders of cyber firms, government and military leaders. In attempting to supply answers to the mounting questions, they recount anecdotes from their multifaceted experiences that bring these topics to life. And illuminate the way forward.

DOWNLOAD FOR FREE



IN FOCUS:

CYBER AND THE BOARD

FROM CYBER CRISIS TO SUSTAINED REPUTATION MANAGEMENT: LEADING COMMUNICATIONS FROM THE BOARDROOM

MELANIE ENSIGN

On June 5, 2013, The Guardian began publishing what turned out to be the first of many articles about the National Security Agency's (NSA) collection of domestic email and telephone metadata. At the time, I was leading cybersecurity communications for AT&T through an engagement with their PR agency of record. The revelation that AT&T had been secretly turning over customer communications to the NSA for years (even behind the back of its own security team) quickly ignited intense scrutiny from journalists, politicians, and customers from around the world. Tensions were high inside AT&T as employees grappled with new information about the company they worked for.

According to news reports, AT&T willingly gave the NSA access to billions of emails as these flowed across the company's domestic networks. The company also provided technical assistance in carrying out secret court orders to wiretap internet communications at targeted AT&T customers, including the United Nations headquarters in New York.

Now, AT&T's security and communications teams were both well-versed in managing security incidents. At the time, AT&T owned the largest global mobile network, giving us visibility into the most prolific as well as the most novel attacks against corporate networks to date. The company was recognized as one of the foremost leaders in defending against the then-exploding threat

of distributed denial of service (DDoS) attacks. Journalists sought the expertise of our security team when covering stories ranging from telecom fraud to nation-state attacks.

But the news cycle in 2013 wasn't about an unauthorized intrusion or coordinated attack. AT&T's systems remained intact and operational. Yet, the NSA revelations completely shut down the company's ability to speak publicly about any of its cybersecurity investments or services without having to address its relationship with government intelligence agencies. All executives and company spokespeople had to be prepared to field press and customer questions about the company's commitment and ability to keep personal information safe. Public skepticism lingered. Our credibility did not.

NSA/AT&T parody T-shirt

Nine months later, at the end of February 2014, things weren't any better. When members of AT&T's cybersecurity team attended a social gathering related to the annual RSA Conference in San Francisco, they were asked by a prominent cybersecurity reporter how they felt about all the parody T-shirts donned by attendees showing the NSA logo with an eagle using its talons to plug into AT&T's network. The response was chilling, and the resulting article caught the attention of company executives. It was clear there was still a lot of work to do to repair the company's cybersecurity reputation.

All of this happened without the presence of a single "hacker," software vulnerability, or compromised password.

A constant cloud of public distrust should concern every executive and board member, not only because of the immediate distraction and costly legal battles it provokes, but also because it makes your brand a toxic affiliation to all the allies you're going to need later on. You've lost reputation capital, and every sale, partnership, or endorsement just became a lot more expensive.

CYBERSECURITY IS A PERMANENT REPUTATION ISSUE: IT NEVER STOPS

Historically, executives and their boards viewed cybersecurity as a crisis communication challenge because they saw it as a one-off or infrequent occurrence. The truth is, very few have had complete visibility or knowledge of just how often incidents occur at their companies. Today, cybersecurity risk and reputation are key components of brand trust. They are significant considerations in B2B contract negotiations and deal-making. Like it or not, they are now boardroom conversations. That's why you're reading about them here.

At the same time, organizations are facing a growing number of new requirements from global regulators focused on consumer protection, securities, and corporate governance. Customers—both business and consumer—expect cybersecurity to be an integral part of the way organizations operate and build products. So, no matter how many cybersecurity incidents an organization must publicly disclose (pro tip: disclose more than you have to), this is no longer a one-off exercise with a clear-cut beginning and end. Rather, speaking publicly about cybersecurity is either an ever-present albatross around your neck or an opportunity to proactively build trust before you need it.

Companies that earn credibilty for their security investments and capabilities receive the benefit of the doubt, even when their overall brand reputation is struggling.

As a member of the board, do you know how your company fares in terms of trust and reputation around cybersecurity and privacy? Are you encouraging proactive and transparent communications from your executive teams to establish trust in how the company treats security investigations, incident response, and customer support? It's not enough anymore to simply ask how the security team is keeping up with the growing threats. Executive teams are also responsible for communicating those efforts to business stakeholders.

Perhaps the most important role of a board member is allocating appropriate resources to cover not only the technical aspects of security, but the human-to-human aspect as well. If your security team doesn't have a dedicated security communications role, create one. Someone needs to be focused on this full-time while the CISO is focused on communicating with you.

Here's another tip worth keeping in mind. Companies that earn credibility for their security investments and capabilities receive the benefit of the doubt, even when their overall brand reputation is struggling. Here's an example. I was leading global security, privacy, and engineering communications at Uber in 2017, when I received an email on Christmas Day from a weekend editor of a popular tech publication who didn't normally cover cybersecurity topics. (I am not naming him because I have no desire to pick a fight or embarrass anyone.) He was calling to fill in the blanks on a story already in the pipeline for publication regarding claims that Uber was trying to stiff a security researcher who had submitted a vulnerability report to its bug bounty program.

This was seemingly a slam dunk, anti-Uber clickbait headline. Bug bounty programs typically pay external security researchers for finding vulnerabilities in an application or system so they can be fixed before they're exploited by an adversary. If Uber was trying to get out of paying a well-intentioned researcher for helping to secure its products, this would have been an easy story to believe and add to the company's reputation for being untrustworthy.

I instantly knew exactly which security issues the editor was calling about because I'd worked with Uber's bug bounty team on their communications with the researcher over the past few weeks. The researcher had violated the terms of our program, provided no information to validate his claims, and attempted to bully a member of our team.

In a matter of minutes, I was able to explain the situation to the editor and refer him to several public comments made by prominent and well-respected security experts from other large tech companies as well as other security researchers who'd seen this man's allegations on social media. They not only condemned the abusive behavior demonstrated in the researcher's correspondence with our team, they acknowledged the professionalism and accuracy of our security team's response.

The article still ran (Christmas is a slow news day), but the story was very different now. The editor characterized Uber's response as detailed and professional, while the researcher's behavior was

One of the most common pitfalls organizations make when it comes to managing cyber incidents is to wait for an incident to occur before engaging.

called combative and labeled harassment. I have no doubt this researcher likely has many redeeming qualities outside his engagement with our team, but he hadn't considered how his actions in this situation would help or hurt his own credibility.

For Uber, a cybersecurity story that easily could have become a PR crisis on Christmas, ended with a public gathering of unlikely, unsolicited, yet influential allies. Despite the company's perceived shortcomings overall, the security team demonstrated in that moment that Uber had redeeming qualities as well. We'd considered from the very first correspondence that our response could proactively and positively impact the way people thought about Uber.

Again, there was no breach here, and we could have adopted a reactive approach with a simple company statement defending our position. Being proactive about our security reputation led to the decision to put communication advisors alongside our bug bounty team to guide our engineers—and that gave us more control.

For board members concerned with the impact of security issues on external perception, it's a good exercise to ask how security communication plans extend beyond mandatory disclosures to build goodwill and establish allies in advance of the next security incident. Ask for communication-specific tabletop exercises and note where the business needs more reliable relationships, intel, and experience to help steer the outcome.

BUILDING TRUST WITH PROACTIVE COMMUNICATION: DEMONSTRATE HONESTY AND COMPETENCE

So much of what a CISO does is focused on communicating the impact of their team to the business. Why not turn that on its head and ask how they're educating external stakeholders like business partners, customers, and regulators about all the work they're doing to be trusted stewards of data, shareholder profits, and consumer safety?

In cybersecurity, trust is earned by consistently demonstrating two things well: honesty and competence. Poor execution is enough to invalidate good intentions. These are familiar principles for corporate communication teams, and they have even more importance for long-term credibility issues like cybersecurity that build on all previous incidents. The statement, "Security is our top priority" is rendered meaningless when accompanied by a notification that an organization's security systems failed to protect its clients and/or customers.

If security is, in fact, a top priority, why are so many organizations scared to talk about it proactively? Could it be that it hasn't truly been prioritized by the business to the extent we want people to believe? Is it not the role and duty of corporate communication professionals to advise organizations on how to close the gap between perception and reality by helping them become who they aspire to be? If security is not the top priority, don't say it is. If it should be, dust off your powers of persuasion in order to make that statement true.

During my time at Uber, giving conference talks and writing blog posts was very popular among our engineering teams. It was a critical part of the company's culture for technical teams to exchange experiences and learnings with peers in the industry. Solving shared technical challenges and adopting best practices delivered net-positive results for everyone. At the same time, I knew that if the public believed we lagged behind in basic application security practices, we'd never have the credibility we needed to be given the benefit of the doubt if a serious incident occurred. We needed to build credibility in advance.

So, I implemented a requirement for engineers to close all security tickets assigned to them before seeking approval to publish a blog post or speak publicly about their work. After all, why would we bring more public attention to products or areas of our tech stack that we knew had vulnerabilities or security weaknesses? I couldn't honestly tell anyone that security was a priority if we weren't even holding software creators accountable for their products. The end results were a shorter lifetime for vulnerabilities in our code, less time spent responding to media inquiries about bugs found by external parties, and more time for telling our security story proactively, on our terms, with the proof to back it up.

The second element of trust, competence, is where corporate communication teams often feel less comfortable. That's why support and encouragement from the board are so important. Publicly sharing details about technical cybersecurity work often requires more than surface level subject matter knowledge. You may need to convince more risk-averse colleagues, like legal or PR compatriots, to engage in proactive communications as well, and that is often out of their comfort zones. Understanding where your organization's risk tolerance intersects with cybersecurity best practices is a helpful place to start, showing that even if your organization isn't (yet) leading the pack on cybersecurity innovation, at the very least you're aligned with industry standards.

Proving honesty and competence means avoiding hype, misrepresentations, or false statements. Many costly cybersecurity and data privacy settlements between private sector companies and the Federal Trade Commission (FTC) start with inaccurate statements on websites or marketing materials. If you can't prove it, you probably shouldn't say it at all. And if you want to say it, especially if you know it will help in the event of an actual cyber crisis, then prove it first and publish it now, so it's ready when you need it. For example, if your organization requires customers to create user accounts, confirm your organization is following best practices for multifactor authentication and make that information available on your website.

PREVENTING CYBER INCIDENTS FROM BECOMING A CRISIS: A LESSON ON INCENTIVES

One of the most common pitfalls organizations make when it comes to managing cyber incidents is to wait for an incident to occur before engaging. A traditional crisis communication approach may offer helpful principles for responding to an incident after the fact, but it lacks structure for preventing or minimizing incidents in the first place. The corporate communications function has valuable skills and organizational visibility to guide a business away from a disaster, so simply waiting for a crisis to occur is a dereliction of duty. And if they're paying attention, directors can make a difference. As a member of the board, it's important to understand that expressing your expectations for security communications goes a long way in determining which approach the communications team will take.

There are best practices for technical security teams to harden their potential attack surfaces. It's expected that an organization serious about security would consider potential risks throughout product development, employee onboarding/offboarding, and supply chain relationships in order to prevent avoidable incidents from occurring. The same should be true for corporate communications teams. We can help organizations minimize or completely avoid incidents that escalate to the point of crisis.

For example, multiple U.S. tech companies have been fined and sued for misleading users about how their contact information collected for account security would be used. Both Facebook and Twitter were issued hefty fines from regulators in recent years for using telephone numbers for targeted advertising that were provided by users specifically to enable two-factor authentication. While their PR teams insisted for years that this information was only used for security purposes, the truth is that they didn't really know. They weren't engaged deeply enough in the day-to-day work of the business to adequately ensure the accuracy of long-held assumptions, and they weren't notified when things changed.

The most common inquiries I received from journalists during my time at Uber were about credit card fraud—consumers seeing Uber charges on their credit card that weren't showing in their trip history. The volume of media questions about this topic easily outnumbered questions about advanced cyber threats 10:1. This was an important factor for consumers in deciding whether they could trust the security of Uber's platform overall, and I wanted to provide a compelling rather than a defensive answer.

How an organization responds to an incident has a greater impact on its reputation than the incident itself.

This led me to develop a close partnership with Uber's anti-fraud and account security teams. We developed a reliable process for confirming the accuracy of every claim brought to us by the media. (More than once I had to break the news to a reporter that it was actually their own teenager who was using their account, not a hacker.) We were able to influence critical product decisions that increased consumer security and provided a compelling response for media inquiries, such as how much personal information should be visible in a rider's account. Credit card numbers were not shown in the mobile app or web account, so fraudsters couldn't steal that information by hacking into individual user accounts. That message resonated with media because it dispelled a common myth and demonstrated we'd thought proactively about consumer security.

As a result, many of these stories simply died on the cutting room floor. Few reporters at the time wanted to report a positive story about Uber, and the stories that did survive became opportunities for us to talk about our security investments and build trust in the platform. Over time we added even more anti-fraud capabilities, such as blocking credit card numbers stolen from other platforms or services from being used on Uber's platform. Every time, it was an excuse for me to engage with investigative and consumer protection reporters and give them another reason to fact-check their next "gotcha" story. Our team even became go-to experts for questions journalists had about the security of our competitors' platforms because their corporate communications teams couldn't (or wouldn't) respond with the same level of detail and concern that we did.

WHEN SH*T HITS THE FAN: PREPARING FOR THE WORST

How an organization responds to an incident has a greater impact on its reputation than the incident itself. The emotion solicited by your response will linger even after the details are forgotten. This includes the technical detection and remediation efforts as well as internal and external communications. A proactive cybersecurity communications strategy aligns with an organization's technical playbooks to consider how public perception impacts—or is impacted by—potential security threats.

For example, vulnerabilities discovered in widely used open source packages simultaneously affect thousands if not millions of organizations. If you're exposed, you're usually one among many and, so long as your technical response is sufficient, you may not experience any public attention for being vulnerable. If, on the other hand, you're the victim of a targeted attack, there are fewer relevant voices to satisfy the media's appetite. If you don't engage, the possible alternative sources will be far less informed, and thus, less accurate. They may or may not give your organization any credit at all for the efforts you made to prevent or minimize damage, or for how well you responded.

Being proactive gives your organization more options and resources for minimizing or eliminating the impact of a potential incident. I mentioned earlier how valuable it can be to have important information prepared in advance. It's impossible to include all relevant context and justifications in media statements or customer notifications. There simply isn't space. News outlets will not quote a five-paragraph essay, so if you want additional information to be considered by your most important stakeholders, you have to create a home for it and establish a norm for sharing information in this way.

Many engineering-first companies maintain network performance websites where they report updates on any service outages. This is a good model for conditioning customers and media to look for more information beyond what's in your media sound bite. These details matter because, over time, this is how you build credibility before something happens.

Keeping this information up to date is critical. As your technical systems change, so should your public content. New products and features under development should have a security story to accompany the launch, explaining how you addressed any potential security risks. Help your technical teams share their learnings with their peers, not just their cutting edge work. This is how you earn informed allies (perhaps even unexpected ones) who can speak up for you when needed.

Finally, consider how closely your response plan follows your day-to-day escalation path. A playbook that only gets used once in a while gets dusty and requires more cognitive effort to follow. Playbooks and plans that don't evolve with your organization are quickly abandoned when situations become intense. I prefer response plans that mirror daily operations as much as possible with appropriate escalation triggers based on severity and legal requirements.

If corporate communications wants to have oversight and input on what is said to various stakeholders in an incident notification (because someone will share those messages with media), then they need to be engaged in ongoing security communications with stakeholders. A breach notification shouldn't be the first introduction stakeholders have to your security team. That's how crises happen.

Melanie Ensign *is the CEO of Discernible, a cybersecurity and privacy communications advisory firm. She is Co-Chair of the Privacy Workforce Public Working Group at NIST and the former Press Department Lead for Def Con. She previously worked in communications at Facebook and Uber.*

WHAT SHOULD A BOARD UNDERSTAND ABOUT AI?

DR. EDWARD AMOROSO

The governing role of the board member is generally well-defined, but often misinterpreted by observers. So let me start with a reminder of what corporate board members are expected to do. First, they must participate in reviewing and overseeing management. This requires the skill to know when and where to chime in, and this is easier said than done.

Second, they must participate in corporate strategy to help drive the company to an optimal decision when something truly consequential is being considered. Major mergers and acquisitions, for example, generally demand the attention of the board, but minor, day-to-day management decisions do not. Again, the principle sounds easy but sticking to it in practice is not..

Finally, corporate board members are expected to review and ensure the accuracy of important financial statements and other key data reported by the company. This does not imply using a fine-toothed comb to review every ledger item, but it does require active enough participation to ensure that public reporting is correct.

In addition to these responsibilities, board members frequently find themselves wading into new areas of concern that their companies confront. Cybersecurity is one such area that has spurred considerable debate about whether directors should play a significant role in making decisions, and if so, how involved they should be. Certainly, they are not expected to be security experts, but general agreement exists that broad awareness is now necessary.

Business leaders will obtain guidance on future trends in the same way a radiologist can work with AI to view data and create accurate interpretations.

A comparable issue involves artificial intelligence (AI). In recent months the public dialogue has been intense (to say the least). You can be sure there have been innumerable private conversations behind closed doors. What are AI's implications for the business? And by the way, how will it affect security? Just as corporate directors are not expected to be experts in that field, they are not expected to be experts in AI. But a consensus is emerging that it is a key aspect of a board's responsibilities.

That said, what are the key considerations for board members on this subject? What should they know about the business implications and security implications? How much do they need to understand about this important technology?

BUSINESS IMPLICATIONS

The effects of AI on business will differ from one industrial sector to another, but some general statements can be made. Hopefully, these broad characteristics in the context of modern business will start the intellectual process for board members to begin integrating AI-related impacts to their governing responsibilities.

Below I've listed issues with an emphasis on how they relate to boards. I've skipped over those that might have a substantial impact on business but not on board responsibilities. Please keep this in mind. My guidance here is for boards, not day-to-day executives and practitioners.

Business Writing Will Become Software-Defined

Board members should recognize that for many years the quality of normal business writing has varied considerably. I'm talking about the memorandums, policy statements, agendas, meeting minutes, and other narratives that have been used in business for decades.

The problem is that so much of this writing has been just terrible, often including nonsensical reports, lengthy papers, and unclear narratives. Board members are certainly familiar, for example, with the large volume of often unintelligible materials presented in advance of meetings. This is common across all aspects of modern business.

AI will have a direct influence on the quality of these written artifacts because automation is so well-suited to this task. Auto-generated notes after online meetings are already common, and this will extend to a fully software-defined approach to business writing that will have considerable consequence on all forms of business communications. And it should represent a tremendous improvement.

AI Will Drive Business Macro Trend Analysis

Board members and corporate executives have depended for many years on the predictions and observations of trends in the marketplace. These often come from industry analysts who opine based on their admittedly limited view of the many factors that influence any type of prediction.

While there will always be interesting personalities who can provide incisive and even humorous observations on macro trends, the use of AI to analyze market trends will be a more common

occurrence. The advantage AI has is that it can include virtually every factor for which some evidence is available to drive the optimal prediction.

Board members should expect to see a symbiotic relationship between human and automated market trend analysis. Business leaders will obtain guidance on future trends in the same way a radiologist can work with AI to view data and create accurate interpretations.

Customers Will Learn to Accept AI for Certain Applications

The ongoing debate with respect to the suitability and acceptability of using AI for certain applications will gradually wane in favor of societal acceptance of the technology. This happens for every new technological advance, including early industrial advances as well as the advent of computing.

The implications for board members is that aggressive adoption of AI, where appropriate, is the best course of action, and hesitation related to concerns about societal qualms is not recommended. Certainly, regulation and some degree of control will be required, but I advise businesses to be aggressive.

The first obligation that every board member should recognize—and this point should be patently obvious—is that a basic working knowledge and baseline understanding of AI is a requirement for modern board members.

SECURITY IMPLICATIONS

The security implications for any type of business will involve offensive considerations ("Can we be hacked by an adversary using AI?") as well as defensive considerations ("Can we use AI to protect ourselves from an adversary?"). As one would expect, use of AI for both is an obvious corollary.

Below I lay out key security-related issues that emerge for board consideration. These should be addressed and coordinated across the entire management chain, and that should include the chief information security officer (CISO).

Major Adversaries Will Use AI to Attack

An important recognition that every business must understand is that their country of origin will certainly be targeted by nation-state adversaries using AI-based offensive measures. Organizations located in the United States, for example, should expect that countries such as China and Russia will most likely develop and use these methods.

The implication from a corporate perspective is that the front line for cyber threats is not the military or even the government, but rather is the distributed collection of data from business, enterprise, industrial groups, families, individuals, and other non-government targets. This is where an adversary nation will target with cyber threats.

Countries Will Need AI to Protect Infrastructure

Special consideration is obviously needed in protecting critical infrastructure, if only because the consequences of an attack can be so much more severe than attacks to other sectors. For board

members with responsibility to manage critical and essential services, the need to maintain secure defenses against AI-based smart attacks will be paramount.

An implication of the existence of AI-based offensive cyber methods is that organizations will need AI-based defensive measures to put a reasonable protection in place. It should be obvious that if an automated attack is being levied, then the defender will not be able to stop such an attack merely by using manual, procedural methods.

Board members should be cognizant of major investments in AI-based security infrastructure, not to review or approve the specifics of the technology or vendors selected, but rather to ensure that a strategic plan is in place to maintain the ability to stop these new forms of attack with a solid AI-based protection scheme.

Social Engineering Will Benefit from AI

One attack that all board members will be familiar with involves the use of social engineering tactics to trick an individual into sharing sensitive information or to perform inappropriate tasks such as transferring money from one account to another (e.g., through fake text or email to a finance officer).

The foundational basis for social engineering involves skill to take advantage of the trust of a targeted person, and this requires having information about that target. Since AI is so good at collecting and analyzing information to establish context, it should be expected that social engineering, including phishing, will become more difficult to stop.

As with nation-state attacks, social engineering attacks will also demand a strategic plan to ensure proper protection. Boards should monitor their companies' defensive programs and should request to see evidence that these are working. Past methods, such as phish testing, will be useful components but will not be sufficient as the basis for such protection plans.

BOARD OBLIGATIONS

The first obligation that every board member should recognize—and this point should be patently obvious—is that a basic working knowledge and baseline understanding of AI is a requirement for modern board members. I wrote this article with this initial goal in mind.

In addition, however, there are emerging tasks that should become part of the day-to-day board ecosystem. While these tasks will evolve over time, let me point out a few below that I expect to see become important in the coming years. Local business conditions should certainly be used to tailor these general points.

Mergers and Acquisitions Must Include AI as a Factor

If the organization regularly performs mergers and acquisitions (M&A), then it must become a standard component of the evaluation rubric that potential AI disruption be considered. The last thing any organization needs is to make a major investment in a company that will soon be disrupted or even replaced by AI.

The M&A team should be directed by senior leadership, with governance from the board, to ensure that this factor is thoroughly considered, especially for mergers that are sizable with consequence to the firm. Without such careful scrutiny, the possibility of a poorly conceived merger or acquisition seems possible—and potentially disastrous.

Human Decision-Making Will Not Be Replaced by AI
A commonly stated point in the popular media, and one that might have some influence on board member thinking, is the claim that AI will replace human decision-making. This may be true in certain situations where data is perused and processed in a structured manner. Radiologists, for example, might replace certain of their data tasks with AI.

The suggestion, however, that this will occur in the context of board strategy, corporate governance, and organization oversight is not reasonable. Good board governance will make use of technologies such as AI to ensure optimal context for discussion and debate, but robots are not likely to gain a seat at the board any time soon.

Cost Reductions Can be Considerable Using AI
One advantage that AI does bring to most business contexts is the ability to reduce cost. Customer care, help desk support, and other tasks that involve procedural steps will be good targets for such reduction. And boards would be wise to establish oversight where such cases are being considered.

The goal, obviously, should be to balance the needs of the firm for cost optimization with the needs of customers, who will demand high quality interactions, and also the needs of employees to feel safe that their career paths will be preserved—or at least guided toward areas that will complement the use of advanced technologies such as AI.

ACTION PLAN

The best course of action for corporate boards and individual board members may have already begun with perusal of this article. Education will be a key differentiator between boards, and any governance team that takes the time to learn the implications of AI will have a clear advantage.

My advice for an action plan is to over-index on education and training. The steps implied by the comments above should be included in local planning, but each organization is different. In the coming years, board members will have to earn their paychecks by developing effective plans for governance and oversight in this new technological era.

Dr. Edward Amoroso *is the Founder and CEO of TAG. He is also a Research Professor at NYU's Tandon School of Engineering and the author of six books. Before he retired to start his own company, Amoroso was the SVP and Chief Information Security Officer for AT&T and a member of the Board of Directors for M&T Bank.*

A STRONG MANAGEMENT-BOARD PARTNERSHIP IS CRITICAL FOR A COMPANY'S CYBERSECURITY

ANNE CHOW

Over the years I've worked with an array of business leaders in the context of their strategy, digital transformation, customer and employee experiences, and use of technology. In all cases, one of the greatest challenges they've faced is the complex, ever-changing, unpredictable nature of the environment. No doubt this is due to imperatives such as the need to dynamically access global talent pools, broaden partner ecosystems, and diversify supply chains while harnessing powerful emerging technologies and new innovations. The continued expansion of the digital landscape around the world, increasing the depth and breadth of the "connectedness" and "intelligence" of organizations will, by definition, result in greater exposure to vulnerabilities, risks, and threats.

Cybersecurity is relevant to all of this, for every business. "Cyber everywhere" is a reality, going far beyond the walls of an organization. It's now relevant to a company's entire infrastructure and ecosystem, touching their plants, mobile and remote workers, connected devices (which propagate vast amounts of sensitive data), as well as home and company networks. It's estimated that by the year 2025, damages from cybercrimes will hit $10.5 trillion annually.

A CEO, no matter how competent and tech-savvy, can't counter these challenges alone. Not even with an excellent management team. It takes an all-company effort. This obviously includes the chief information security officer (CISO) and the IT department, but it doesn't end there. It's important that the board of directors is engaged and involved, and works in cooperation with executives. If one component of a company simply defers to another to create and implement the cybersecurity strategy, the engine is not firing on all cylinders. "Cyber everywhere" requires an all-hands defense—and offense.

I've learned a lot about this over the years from experiences as a senior executive and as a board member. I started from a pretty good perch. As a second-generation telecom professional (also known as a "Bell Labs baby"), it seems I was destined for leadership roles that placed me at the intersection of technology and people. When I entered the industry in 1990, with degrees in electrical engineering and business, I was a fledging network engineer. My earliest notions of cybersecurity at that time were about computer viruses and bad people trying to hack into private, often mission-critical, systems. From my early vantage point, protecting the network—that of my customers and company—was paramount.

Then, seemingly overnight, the world became connected with explosive internet-catalyzed innovation. The accompanying solutions and growth transformed the experiences of consumers, communities, businesses, governments, and society as a whole. In the three plus decades that ensued, I held numerous leadership roles with increasing responsibilities in telecom and technology that focused on the business marketplace across many areas, including product management and development, marketing, strategy, customer service, operations, and sales. In 2019 I became CEO of AT&T Business, a global $35 billion operating unit with 35,000 employees serving business customers with a full realm of technology solutions. Cybersecurity was mainstream and relevant to all facets of an organization by then—no matter the industry. AT&T had its own portfolio of services and partnerships that helped customers safeguard their network security. In fact, one of my mantras for my team, when it came to our customer relationships and services, was: *Connect … Protect … and Respect.*

While at face value cybersecurity may appear to be a technology issue, it is not. It is, and forever must be, a priority business issue for all boards and senior management teams.

In addition to my operating executive roles, in 2016 I had an opportunity to join my first public company board. To this day, I still serve on this small cap board, now as the lead independent director of FranklinCovey, a leadership, development, and training company. Later I also joined the board of the well-known global conglomerate 3M. With my additional perspectives as a director, I've grown particularly passionate about the relationship between executives and their boards, viewing it as vital to an organization's success, no matter the company's size or sector. And a lot of that is due to the impact of cybersecurity. It's a domain that is perpetually evolving. Perhaps that's why clarity on the board's role in partnership with senior management is elusive and often fluid.

Several years ago, at a board director summit whose participants hailed from different industries

across the private and public sectors, I heard a common sentiment from fellow board members: "Cyber risk is well managed by the IT team." Even if the statement is true, it leaves me unsettled, given my knowledge of and experience with the threats, risks, and vulnerabilities that businesses face—whether they are aware of them or not.

The roles of a board are not limited to strategic planning, leadership governance, and oversight of CEO evaluation, succession planning, and executive compensation. They foundationally include the fiduciary responsibility to protect and grow shareholder value responsibly. While at face value cybersecurity may appear to be a technology issue, it is not. It is, and forever must be, a priority business issue for all boards and senior management teams.

Cybersecurity and geopolitics have become inextricably linked. As boards work to navigate geopolitical risk, cyber must be part of their scope. Unfortunately, the world of technology has in and of itself become political, which further exposes global businesses, especially across interconnected supply chains, to escalating levels of threats.

No doubt each of us has been subject to phishing attacks, and businesses are constantly being bombarded with various social engineering tactics by bad actors seeking to gain access to sensitive information. Ransomware attacks are on the rise, with extortion techniques evolving in sophistication and impact. And the unprecedented, exponential advancement of generative AI serves as an accelerant to the flames of cyber risk on an ever-growing attack surface. Let us also acknowledge that AI will fuel innovations from both the "good guys" and "bad guys," compelling us to always be wary about what's happening around us.

Management's efforts to mitigate strategic risks is a key area of collaboration between executives and boards. In the case of cybersecurity, this must be handled with both proactive and reactive plans. Meaning, management must ensure that their boards understand:

- What the company is doing to identify risks based on their view of the greatest vulnerabilities, and what is being done to protect the environment, including both physical and digital assets. Of particular interest are what controls and protocols are in place from a human perspective, as in this mobile, hyper-connected world, people (whether employees, suppliers, partners, or otherwise) are often the weakest link. This includes identity management, verification, and authentication of not only people, but also processes, system handshakes, and more.
- What the company is ready to do if an incident occurs—how they will detect it, respond, and ultimately recover. This includes not only recovering from the incident itself, but remedies developed from root cause analyses to prevent future exposure. It is vital for the board and management team to be on the same page of the incident response playbook. This playbook must be comprehensive enough to cover the roles of all key players. It must also recognize that the operational teams involved in the incident management cannot be expected to simultaneously manage stakeholder communications. A systematic approach to customer communication must also be a critical element of the plan.

THE ROLE OF THE BOARD

Boards must understand what their role is—in times of crisis as well as in a steady state. Oversight, governance, and risk management require a focus on several key areas to enable shared accountability for cybersecurity with executives. When I work with senior leaders, including those who serve on boards, a common concern I hear is, "I'm not that technically fluent and don't fully understand cyber." One does not have to be a technologist to learn about the cyber world, and more importantly, what the implications are to the business an individual is responsible for. As

with any area of concern—geopolitical, regulatory, environmental, social, legal—the board's role is to strategically connect the dots, working hand in hand with management.

Here are some of the questions board members and senior management need to consider:

Traditionally, boards have viewed cybersecurity as the responsibility of the audit committee. But the understanding and insight required often exceed the expertise found on most of them.

Context and Critical Resources: What is the strategic context and framework for how the business views cybersecurity? What explicit and implicit linkages exist between the company's overall infrastructure, cyber ecosystem (hardware, software, network, people, data), and critical business success factors? How are data, data protection, and cyber integral parts of the organization's business strategy, value proposition, and competitive differentiation? What is the holistic enterprise level view of cyber? Do we have sufficient cyber talent on hand? Do we have a cyber-clear culture where our team members understand what's required of them to do their jobs in a secure way? Do our people know what exposures to be aware of? And do we "test" the cyber rigor of our processes and resilience of our culture?

Metrics and Measurements: What are the right metrics for the board to understand? What operational data are provided to the board (which could include efficiency, effectiveness, regulatory, and compliance-oriented metrics)? What does the data mean? Beyond traditional red-yellow-green scorecards that indicate degrees of risk, what do trend results tell us? Do we know where we have the greatest exposure—strategically, operationally, and technically? And are we sufficiently investing in resources, technology, and partnerships to mitigate and manage the concerns? Do we understand what our most valuable assets are, and do our measures and methods help us protect and secure them? Do the answers to these questions create the need for a small set of enterprise-wide board level metrics which supplement the operational ones?

Education and Expertise: What base knowledge should the board understand? Not necessarily deeply technical, but information that links the technical to business implications? What cyber fundamentals feel vital to use, such as the NIST cyber framework, and how do we ground ourselves in where we are rather than where we should be? Is this an area of strength or weakness for us? Do we have a cyber-oriented culture not only in the company and across the management team, but also at the board level? How do we sustain it?

Communications and Governance: How frequently should we be communicating with the board on our progress? How do we utilize board meetings and committee meetings in these updates? Do we have a robust crisis management process and incident playbook, tested periodically with tabletop exercises? These exercises must include post-breach protocols; use of outside counsel and forensic consultants, as appropriate; communications with key external stakeholders, such as the FBI; and potentially, board involvement. Are we bringing in outside and industry experts on a regular basis to ensure that we have the most current thinking on threats and opportunities going forward?

Speaking of governance, I've also heard the following from board members (from both publicly traded and privately held companies): "There are board members who have cyber experience, and I'm counting on them to represent me." Unlike when you're in an operating role and have clear domain and/or functional responsibility, as a board member your responsibilities span the enterprise. High-performing boards collaborate actively across all strategic priorities, which helps to elevate

perspectives and enhance collective decision-making.

Yet, traditionally there has been a belief on boards that "cybersecurity is the responsibility of the Audit Committee." Review and management of the topic has been done in the context of enterprise risk management. However, the understanding of cyber risks and the strategic insight needed to manage them go far beyond the typical financial breadth and depth of expertise found on most of these committees. Alternatively, some companies have moved to establish separate cybersecurity committees and/or IT/Technology committees where cyber is in scope. Leading the way are financial services and health care corporations. Some organizations have even begun treating cybersecurity committees the way they do Internal Audit, giving the CISO/CSO/CIO not only direct access to the board and committee chairs but even direct reports to the board via the appropriate independent director committee chair and a tight partnership with the general counsel (given the expanding legal liability).

From a management standpoint, it is vital not to use a technology-first or technology-only approach when working with the board on cyber.

More and more companies are placing CISOs or executives who have direct operational and technical experience in the cybersecurity arena on their boards to ensure a diverse range and depth of expertise. As a Nominating and Governance Committee chair myself, I can vouch for the power of such diversity when it comes to effective board succession, development, and planning.

WORKING IN PARTNERSHIP WITH MANAGEMENT

On July 26, 2023, the SEC adopted new rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by public companies. Foreign private issuers are also required to make comparable disclosures. The basis for these new rules is the commission's observation that cybersecurity threats and incidents are a growing concern to public companies, investors, and the market. This is a regulatory affirmation of the risks that have increased given global digital transformation. While disclosing a material cyber incident is not a new requirement, what's new about this latest rule-making is the specificity of what, how, and when. This places an even greater emphasis on a common understanding and definition of what is material prior to any actual incidents occurring, understanding that the expectation is that materiality is based on whether the issue is important to investors today and/or potentially in the future.

While the dialogue about these new rules is active and ongoing, there is no question that the roles of the CISO, CIO, and CTO, in partnership with their general counsel and chief financial officer, have become even more critical, given this development. The SEC rules underscore requirements for reporting on management's role in handling these cyber risks, and the board's role in oversight in the face of a growing threat landscape. Timeliness and agility become even more critical. Orchestrated communications led by management across key stakeholder groups must ensure board awareness and alignment.

The board's strategic scope includes the full span of business, technology, regulatory, and market realities. It must be equipped to understand the strategic threats and vulnerabilities to the business that could negatively impact the company's value, both in the short and long term. Its focus is oversight, however, and it must not overstep into the operational realm of decision-making. Management must own all operational responsibilities, working to establish the measures and metrics along with the necessary assessments and audits required to mitigate and manage these risks.

As part of this responsibility, management and board must work together to ensure that the board is devoting sufficient time to the company's technology strategy, operations, and investments. Capital allocation, including optimizing ROI, in the context of strategic imperatives, which improve the customer and/or employee experience, are vital to the competitive differentiation of the company's products and services. Understanding the role of cyber is key to ensure that the appropriate investments are made, including resources dedicated.

From a management standpoint, it is vital not to use a technology-first or technology-only approach when working with the board on cyber. There should always be a business and strategy lens placed on the discussion, including financial dependencies and stakeholder concerns as applicable. When reviewing risk, the conversation should focus on business outcomes and impacts, including contingency plans. In today's digital world, a base level of technical fluency should be expected from the board and senior management team, and the importance and relevance of data must be part of their shared base level understanding—whether it be customer, employee, operational, financial, or other data. An explicit understanding of the greatest vulnerabilities and risks, including potential financial impacts, is required of both board and management teams. And in the inevitable need for prioritization of investments, tradeoffs must be clearly understood.

The downside is significant if cyber is not embraced in this partnership. Not only are there the costs of cyber breaches, which can be monumental, there is also the potential for litigation and reputational losses. At the core is the operational functioning of the organization, which, if disrupted, especially for a significant amount of time, can have severe economic, community, and stakeholder impacts. Whether the breach occurs in a government organization responsible for commerce, a banking institution that plays a key role in global financial markets, a city's transportation infrastructure, or a group responsible for a major energy grid across a large metroplex, the impact of a cyber incident can range from negligible to minimal to moderate to severe to devastating.

THE BOTTOM LINE

In a data-first world, cybersecurity vigilance is a must. This steadfast attention, including controls and compliance, must be owned as a joint responsibility between the senior management team and the board—each with clear roles and a clear understanding of the issues. Systemic, periodic, and ad hoc communications are all critical to the success of the enterprise. There are no guarantees in the world of cyber, but strong alignment and commitment coupled with a collaborative team approach are the best equation for a company to prevail.

Anne Chow *is Lead Director of FranklinCovey's Board of Directors, a Director of 3M, and a Senior Fellow and Adjunct Professor of Executive Education at Northwestern's Kellogg School of Management. A best-selling author, Chow is the former CEO of AT&T Business and was twice featured as one of Fortune Magazine's Most Powerful Women in Business.*

WHAT I NEEDED TO KNOW ABOUT CYBERSECURITY AS A CEO AND LATER AS A BOARD MEMBER

ANDY GEISSE

As the CEO of a startup, my first experience with cybersecurity was … missing in action. There was no experience. My "IT department" consisted of a contractor who ran our server and reported to the CFO. This was in the 1990s, before the internet transformed business. We had PCs, we had systems that those PCs connected to, and we even had email! But we were not familiar with the term "cybersecurity." Most of our employees had one password they used for every system, and you'd be surprised how many desks you could walk by and see those passwords posted. Security never even occurred to us.

A couple of years later, as the CEO of two different startups in Chile, my cyber discussions with the boards, with the chief information officers (CIOs) who reported to the CFOs, and with management were remarkably similar. There were none. The same was true when I was the CEO of a cellular company in New York. We never discussed it at the CEO or board level. Our IT team was expected to take care of it and keep us safe. It went without saying.

Little did I suspect that my first real experience with cybersecurity would be in IT itself. I was asked to run the software group for a Fortune 500

company with a worldwide programming staff that supported over 4,000 applications. I quickly learned that most of the conversation in application development is around functionality for the business and how to do more with less. Security was an afterthought. Usually the security team would come in and do app reviews and point out the holes we had and where we needed to add functionality. Security was never first in the application programmers' priorities.

Things changed abruptly when we were hit with our first major worm right before the turn of the century. It brought down applications across the whole company, infecting many of our systems and servers. We spent the entire weekend, day and night, on calls trying to restore applications and eradicate the worm. We eventually figured out how the worm got in. An employee who wasn't even in IT had attached a server to our internal network and the internet without basic security.

It was an extremely painful lesson in cybersecurity. I was on the phone with the CEO and every top business executive trying to explain something they had never heard of and had no concept of. Yet it greatly impacted our customers, our business brand, and it had a major financial impact. We immediately tried to identify all "rogue" systems inside the company—a task we found to be nearly impossible (and never-ending). We then tried to apply basic security features to each system the various business units had. This was when I started thinking that cybersecurity, far from an afterthought, needed to be considered first.

LEARNING TO TALK ABOUT CYBERSECURITY TO BOARDS

Obviously, a lot has changed over the years. Cybersecurity is a household name. Everyone knows about it, even people who have nothing to do with it professionally and couldn't explain it very well to their children, know enough to worry about it.

Things started changing dramatically for me when I found myself working at a global telecom company with a very experienced chief information security officer (CISO). By this time I was the CIO, and I spent quite a bit of time working with the CISO to understand how we could better fortify our systems, how we could think about security up front in our application development processes, and how we could better manage our own internal security.

When I started meeting with the board, I quickly figured out that they didn't want to know about cybersecurity. They just wanted to know that we were "safe and secure."

That close relationship with tech extended to my next CEO role. I ran the phone company division (consumer and business telecom groups), and eventually I was CEO of the business group. In my new role cybersecurity was not only something we used internally to protect our systems and data, but something my group sold as well. We were responsible not only for our own internal behavior, but for our customers' networks. We were the cybersecurity professionals!

That was when I learned my first important lesson about cybersecurity and boards of directors. When I started meeting with the board, I quickly figured out that they didn't want to know about cybersecurity. They didn't want to talk about it, understand it, or have anything to do with it. They just wanted to know that we were "safe and secure." And they weren't alone. Even my top customers didn't really want to know a whole lot more. They kept asking me "can't you just deliver

a clean pipe," meaning data with no security threats. That was impossible to do. Yet data losses, hacks, denial of service attacks, employee/contractor lapses and intrusions—all of that and more happened daily.

I learned quickly that even if the board and customers wanted to take cybersecurity for granted, as the CEO I could not. I had to work with the CISO to develop a security framework, be able to audit against that framework, and report the results to management and the board. There was nothing worse than having to go to the board's audit committee to explain a cyber threat and intrusion. When we did, we had to have the right reports to explain what we were doing in a way a non-technical board could understand.

Later, when I was a board member, some of the reports I found useful were ones that helped me understand brand and business continuity risks. These included reports that showed us intrusions and how they were being mitigated; loses of customer and employee data and the steps we were taking for each; issues found in the cybersecurity audits and the severity and how they were being addressed. Let me add one more that is often overlooked: reports on employee and contractor cybersecurity education. As important as it is to track security issues, it's also important to track efforts to prevent security issues.

GETTING A BOARD'S ATTENTION

So how do you get their attention? How do you make the board understand that cybersecurity is too important to ignore, or treat as an afterthought? It turned out that news reports were great teaching devices. Some high-profile breaches made a real impression. The **breach at Target** in 2013 was a big one. As many as 110 million customers' data records (40 million credit and debit records and 70 million customer records) were compromised. Target's profit fell nearly 50% in the 4th quarter of 2013. The company lost customer confidence and the stock fell almost 10%. That got the board's attention! I bet it got the attention of most boards. Several leaders in Target's IT department lost their jobs over this breach. Yet it was a hack that was incredibly hard to find. It had gotten in through some contractor clicking on the wrong file. If the right employee/contractor education had been done, could it have prevented this hack?

The 2014 Sony Pictures attack was an event that got the attention of boards everywhere.

Another breach that made an indelible impression was the **Sony Pictures film studio hack** in 2014. It happened shortly before the planned release of a fictional movie about the assassination of North Korean leader Kim Jong-un. It shut down the studio, cost $35 million in investigation and mediation expenses, and erased Sony's computer infrastructure. Above all, it embarrassed Sony with leaked emails about and from executives and stars that turned the mess into a monumental public relations disaster—the kind they make movies about.

What happened to Target and Sony forced boards to sit up and pay attention.

They started to realize the huge impact cybersecurity can have on business continuity, on brand reputation, on market value. And, of course, on customer confidence. This was no longer a "back room audit" issue.

One of my goals was to impress on boards that a major data loss can bring the business to its knees. And the regulatory implications have skyrocketed given the data privacy laws in Europe, California, and a growing number of states. Cybersecurity is not just "an IT issue." I often use examples I find in the press where a company's marketing or human resources department lost sensitive information. The whole company must be aware and involved.

THE CHALLENGE FOR STARTUPS

By the time 2015 rolled around, I found myself facing a new challenge. I was starting to participate on boards of startups. By this time I was an operating partner at Bessemer Venture Partners (BVP), and based on my relationships in the startup world, I began to realize that cybersecurity was not a major topic of discussion at many of those boards. The new companies were so busy building their products, selling their products, raising money—all the things that go with being a startup—that there just wasn't time. Or so they thought.

To sum it up, governance is the key. Especially for startups, because that's often the last thing on their minds.

I was on one startup board where the issue seemed to be handled by the audit committee, which looked at the issue from a risk management perspective. But this audit committee, like others I saw at startups, was filled with former CFOs, who were much more steeped in financials than tech, and really didn't understand cybersecurity or its implications. One of those startups had a major leak of customer information caused by a marketing executive extracting data and putting it on a cloud database to study the analytics. The marketing group didn't have any security at all on the data. Why would they? These were marketing executives, not IT or security folks.

Something good came out of this. The company's leaders recognized they were in over their heads. The audit committee asked me and another board member who had cybersecurity experience to get involved. What we found was typical of startups: there was no CIO, there was no CISO, everything was handled by the product folks who were technically savvy but much more focused on product features and releases. There wasn't a security framework to audit against, no reporting, no understanding of the risks to brand reputation, customer confidence, etc. What made the situation particularly fraught is that this company handled sensitive communications for companies. One major hack could have taken the company down, especially since its service was cloud-based. The whole area of cybersecurity required an entirely different way of thinking.

So what did we do? We set up a cybersecurity committee of the board. We used it to push management to appoint a CIO and a CISO who could report to us the various issues, risks, and mitigation activities. We then hired an outside consultant who helped the new CISO get a security framework we could use to audit against. We ran a complete review of the company using that framework, and we created a list of vulnerabilities and priorities. We established reporting capabilities that would be reviewed each month, looked at actual incidents that had occurred, additional vulnerabilities, and prioritized the mitigation of all those vulnerabilities.

BOILING IT DOWN

To sum it up, governance is the key. Especially for startups, because that's often the last thing on their minds. Startups are all about delivering the product or service. Often for the leaders it feels too early to worry about audit committees and risks. And the board, too, is almost always focused on business results and company strategy. The board doesn't run the company. Its job is governance. It must worry about brand reputation. It's supposed to ask questions and focus on larger issues like strategic alternatives and the company's long-term health.

BESSEMER'S FIVE CYBERSECURITY LESSONS

1. Build a cybersecurity culture.

2. Invest in identity.

3. Secure your cloud and development environments.

4. Manage your data assets and environment.

5. Monitor your third-party risks.

But neither startups nor any other company can afford to ignore cybersecurity. The board should be asking questions about it. I have often done that myself at those meetings, asking management how they measure this area, how they report on it to the board, and who is responsible. The audit committee? A separate cybersecurity committee? A board member who has cyber experience and can do a complete review of the systems with the technical folks and then report back to management?

Sometimes it comes down to this: The board at a startup needs to make management understand that it cannot afford to ignore basic needs, any more than an EV car manufacturer focused on developing a perfect battery can afford to skip the steering wheel. The board needs to communicate to management that today's companies need IT departments and CISOs who can oversee cyber risks and vulnerabilities and report these up the chain. And hire outside talent, if they need to, in order to mitigate the risks. Failing to understand these principles is placing the entire enterprise at risk. And that is the absence of governance.

BUILDING CYBERSECURITY COMPETENCE ON THE BOARD

- **Recruit board members with cybersecurity expertise.**
- **Ensure management has a proactive rather than a reactive strategy.**
- **Develop cybersecurity awareness and knowledge among board members.**
- **Leverage external resources, such as cybersecurity consultants or advisers.**
- **Establish effective communication with the board on this subject.**
- **Utilize clear and concise reporting formats to convey cyber risks.**
- **Encourage proactive reporting of cyber incidents and near-misses.**
- **Conduct regular cybersecurity briefings and training sessions for the board.**
- **Align cybersecurity metrics and performance indicators with overall business objectives.**

Andy Geisse *is an Operating Partner at Bessemer Venture Partners. He sits on a variety of boards and plays an advisory role with a number of companies. He is the former CEO of AT&T Business Solutions, Sr. Executive VP responsible for AT&T's Wireline business, CEO of Startel Communications, CEO of VTR Cellular, CEO of CellularOne in Upstate New York, and CIO of AT&T.*

THE IMPERATIVE FOR CORPORATE BOARDS TO PRIORITIZE IDENTITY MANAGEMENT

JOHN J. MASSERINI

In an increasingly interconnected and digital world, the importance of identity management cannot be overstated. As businesses increasingly adopt distributed cloud environments, head down the path to zero trust architectures, and rely more and more on third parties for critical information processing, the need for adequate access control to protect sensitive information is of the utmost importance.

Corporate boards should be deeply concerned about their organizations' identity management programs, and with good reason. They would do well to study the potential risks and benefits associated with this critical aspect of modern business operations.

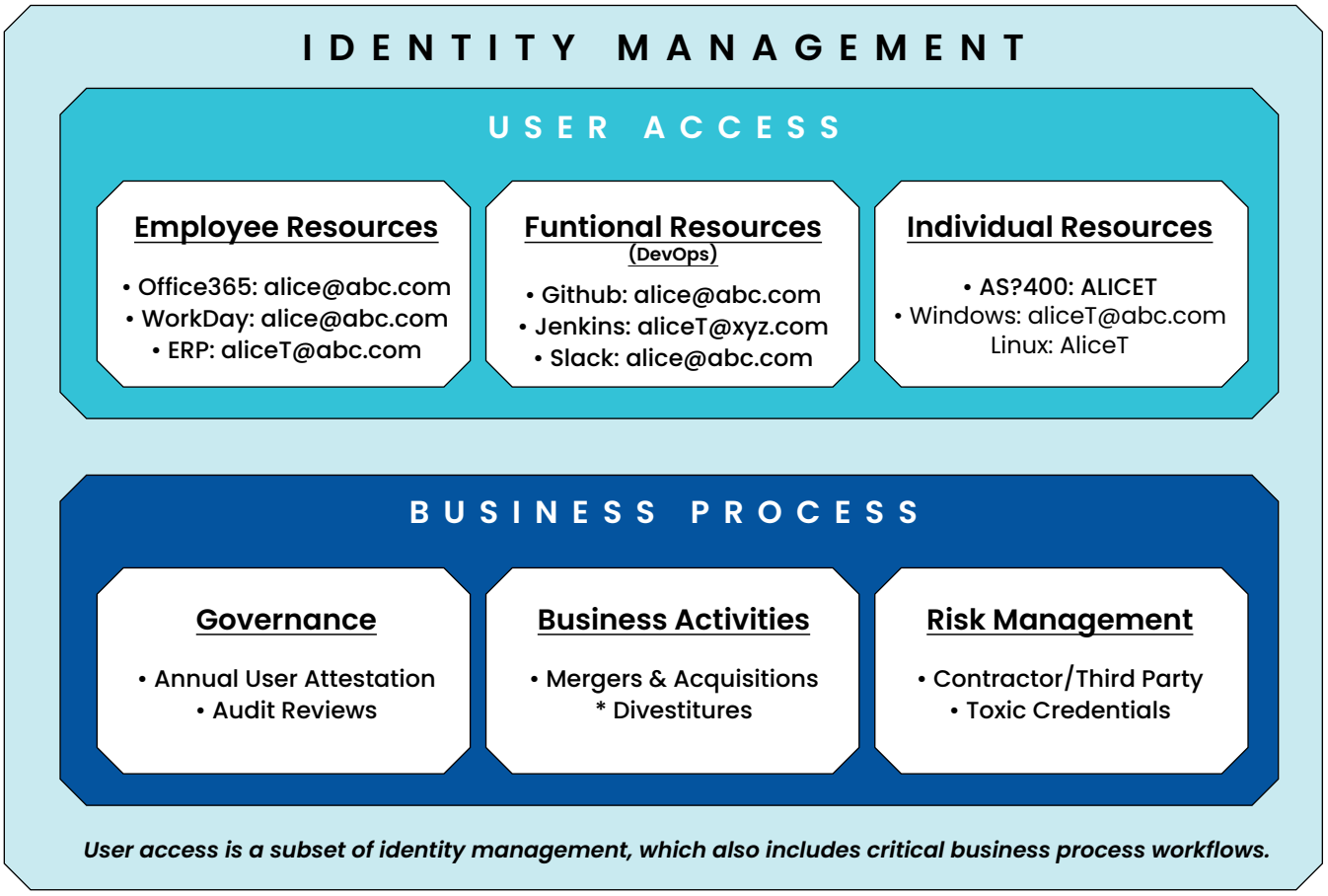
IDENTITY'S EVOLVING LANDSCAPE

Conceptually, identity management includes a broad range of business practices and solutions focused on ensuring individuals have appropriate access to resources within an organization's technical infrastructure. A mature identity management program not only includes the company's employees, but also business partners, customers, and third-party suppliers who may interact with a company's applications and network resources. With

the seemingly endless adoption of cloud computing, mobile devices, and work-from-home initiatives, traditional perimeter-based security models have given way to a more dynamic and varied threat vector.

Unfortunately, most people equate identity management with user access. While similar, it's critical not to confuse the two. Identity management should be considered the overarching umbrella for all user access types, business processes, and maintenance activities that occur in the user ecosystem. User access typically pertains to a specific application or system, whereas identity management is the holistic overview of all user access across the entire infrastructure.

In a mature identity management program, risks can be determined based on user actions and their inherent risk to other systems and environments to which they have access. This holistic view of managing identities by applying risk metrics to user access and activities is what separates companies with well-understood risk exposure from those likely to be the next headline (and not in a good way).



SOURCE: JOHN J. MASSERINI

In reviewing the chart above, multiple components make up an Identity Management Program versus day-to-day user access management procedures. As pictured under User Access, there are three main pillars of functionality:

- **Employee Resources:** These are normal corporate services that every employee needs regardless of job function—the HR platform for benefits (WorkDay), the mail and communications platform (Office365), and the ERP platform for travel and expense (ERP).

- **Functional Resources:** This is an example of a specific team (DevOps) or a functional group's needs within an organization. The DevOps teams need access to their code repositories, ticket and release tools, and communication channels. One could easily replace DevOps with Finance, HR, or Legal, and the appropriate access for those specific teams would follow.
- **Individual Resources:** The access requirements under this pillar are around the specific needs users have in order to perform their job functions. In this case, Alice is a systems administrator, so she has specific "admin" level credentials for some systems. This can also be exemplified, for example, by the differences in access between an accounts receivable clerk and an accounts payable clerk, or a payroll administrator versus a benefits administrator.

When we evaluate the Business Process section of Identity Management, it has little to do with user access but is more focused on governance, business processes, and risk. These verticals break down in the following manner:

- **Governance:** The ability of an organization to prove they are compliant with industry or government regulations is a critical aspect of a mature identity management program. All of the leading regulations require companies to have a solid understanding and control of how users access systems and manage the assigned permissions. This is primarily achieved by consistently running User Attestations, which ensure user access reviews are performed in line with expectations. Similarly, Internal Audit will be spot-checking the attestation process to ensure it aligns with the corporate policies and standards.
- **Business Activities:** Reorganizations, mergers, acquisitions, and divestitures all wreak havoc on technology organizations that are trying to provide a standard level of service to their user population. A well-conceived identity platform allows for easier integrations of new users en masse as well as the selection and movement of departing users. Also, not only does a mature identity platform make IT's job easier, it also provides detailed accountability and auditability—again, supporting those regulatory and audit requirements surrounding the business activity.
- **Risk Management:** While operational efficiency is a key element of a strong identity management program, ultimately it's about mitigating risk throughout the enterprise. Most of today's identity platforms leverage machine learning to identify toxic combinations of credentials that could allow a disgruntled employee or an external attacker access to applications and data they should not have. Additionally, having a centralized location for all third parties and contractors goes a long way in mitigating often overlooked risks in your supply chain.

Ultimately, it's critical to understand that identity management is much broader and much more risk-focused than legacy user access.

RISKS OF INADEQUATE IDENTITY MANAGEMENT

When we evaluate the risk exposure of an inadequate identity management program, it falls into three major categories: data breaches, regulatory compliance, and insider threats. Let's look at each.

Data Breaches: Without robust identity management, companies are vulnerable to data breaches and cyberattacks that can result in significant financial losses, damage to reputation, and legal liabilities. As is often the case, employees tend to use the same credentials across multiple systems throughout the corporate environment. In fact, this is one of the main contributing factors to the substantial uptick in ransomware over the last several years. Unauthorized access to sensitive data

There have been countless examples of insiders disclosing sensitive data—either intentionally or accidentally—and causing a significant impact on a company's reputation and/or market valuation.

can lead to the exposure of proprietary information, trade secrets, and customer data, eroding trust and credibility. This becomes significantly more of a threat as companies move headlong into zero trust architectures which are absolutely dependent on a solid identity management program to be successful.

Regulatory Compliance: Over the past several years, there has been a substantial increase by regulators on how organizations are managing their identities and user access. Sarbanes-Oxley (SOX) audits have become increasingly focused on not just user access, but how identities are managed throughout the legacy infrastructure and within the expansive use of cloud services. With heightened data protection regulations such as the EU's General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA), poor identity management can lead to non-compliance and substantial fines. Additionally, the Payment Card Industry Data Security Standard (PCI DSS) requires businesses that process credit card payments to implement certain security controls, including strong identity management controls. Boards must be aware that inadequate identity management practices could result in severe legal and financial consequences such as fines, sanctions, and long-term regulatory oversight.

Insider Threats: Identity mismanagement is also a key enabler of insider threats, where employees or authorized users exploit their access privileges for malicious purposes. There have been countless examples of insiders disclosing sensitive data—either intentionally or accidentally—and causing a significant impact on a company's reputation and/or market valuation. Whether it's a negligent employee accidentally disclosing information, an employee departing the company and taking sensitive information, or theft of proprietary information, these often-overlooked threats can disrupt company operations, compromise sensitive data, and cause reputational harm.

BENEFITS OF EFFECTIVE IDENTITY MANAGEMENT

An effective identity management system ensures that only authorized individuals can access company resources, reducing the risk of unauthorized access and data breaches. This is especially true in today's modern enterprise, where zero trust, DevOps, and cloud infrastructures are moving critical services outside of the legacy firewalls. Multifactor authentication, real-time, risk-based access controls, and regular identity audits and attestations contribute to a strong security foundation.

By prioritizing identity management initiatives, boards can mitigate numerous technology-centric risks by addressing underlying issues that span the enterprise. A well-implemented identity program enables the identification of potential risks and facilitates proactive measures to address them, reducing the likelihood of security incidents. Additionally, by leveraging modern identity platforms, organizations can leverage AI and machine learning to uncover user-access-related risks that would otherwise be impossible to find.

Proper identity management streamlines access provisioning and de-provisioning, ensuring that employees have the right level of access throughout their tenure. New employees are onboarded

If your organization's revenue stream includes selling services to other companies, being able to demonstrate a robust identity management program instills confidence and trust with your potential clients.

substantially quicker than with legacy approaches, which reduces administrative overhead, saves time, and enhances overall operational efficiency. At the same time, modern identity management platforms provide for employee self-service and requested access when needed with supporting workflows to ensure all necessary approvals are in place. Finally, the de-provisioning process is all-encompassing, disabling access across all platforms and applications with the click of a button. Long gone are the days of abused credentials of employees who left weeks, months, or years ago.

In an era in which trust is a precious commodity, robust identity management can bolster a company's reputation. Customers, partners, and stakeholders are more likely to engage with a business that demonstrates a commitment to safeguarding sensitive information. If your organization's revenue stream includes selling services to other companies, being able to demonstrate a robust identity management program instills confidence and trust with your potential clients. It also goes a long way toward providing SSAE-18 SOC 2 compliance.

By ensuring compliance with data protection regulations such as GDPR, CCPA, PCI, and NIST, boards can avoid potential legal entanglements and financial penalties from both federal regulators and industry associations. A robust identity management program demonstrates a strong belief in corporate accountability and responsibility, helping to build a positive relationship with regulators and auditors.

THE BOTTOM LINE

Supporting and empowering your organization's identity management initiatives achieve not only the mitigation of cyber risk, they also enhance operational efficiency while minimizing the potential for regulatory actions. Corporate boards must recognize that the complexities of modern business demand a strategic and holistic approach to identity management. The risks of inadequate protection are considerable, including financial losses, regulatory fines, and reputational damage. Conversely, a well-implemented identity management framework can deliver enhanced security, operational efficiency, and stakeholder trust.

Here are some parting recommendations for corporate boards:

- Review your organization's identity management policies and procedures on a regular basis to ensure that they are up to date and effective.
- Invest in identity management technology that can help automate access provisioning and de-provisioning, and provide real-time visibility into user activity.
- Recognize that strong identity management should make employees' jobs easier, not more difficult. Haphazard applications of strong passwords and multifactor solutions will only encourage staff to find ways around the controls.

- Integrate identity management into the development/DevOps pipeline to ensure that initiatives such as zero trust and cloud deployments are addressed.
- Automate annual identity attestations, ensuring that responsible managers can easily identify risky access credentials that could potentially cause harm.

Unlike other cyber risk initiatives, identity management crosses the boundaries of the security, technology, legal, and compliance groups. The board must collaborate with the leaders of all of these areas to ensure adequate attention is being placed on identity-related initiatives. Corporate boards should educate and train themselves on not just the impact of identity management on their organizations, but general cybersecurity topics as well. Government organizations such as NIST, NICCS, and NCSC offer board training presentations, and independent organizations such as the National Association of Corporate Directors (NACD) and the Corporate Governance Institute offer formal cybersecurity training aimed at corporate directors. By prioritizing identity management and allocating appropriate resources, boards can demonstrate their commitment to protecting the interests of the company, its stakeholders, and its customers. At a time when data is the lifeblood of the enterprise, and breaches can have profound and far-reaching consequences, the impetus for corporate boards to concern themselves with identity management has never been more important.

John J. Masserini *is a Senior Research Advisor at TAG Infosphere. He is a 30-year security veteran and was previously the Chief Information Security Officer for Millicom (Tigo), MIAX Options, and for the Dow Jones Corporation.*

"Nice idea to soften up the auditors, Karen."

WHAT BOARDS NEED TO KNOW ABOUT CYBERSECURITY TO MEET THEIR FIDUCIARY DUTIES

DEBORA A. PLUNKETT

The fall of 2013 was ripe with almost daily reports of malicious attacks against a myriad of companies, touching businesses across many industries and sectors. These attacks, largely of the distributed denial of service (DDoS) variety, not only interrupted business operations but began to instill insecurities in those who worked at these businesses. It appeared to be the start of a rash of incidents that impacted the banking and retail industries as well as government organizations.

As the deputy director of information assurance for the National Security Agency, my job was to develop and deliver security solutions to protect national security systems, largely defined as classified data and networks as well as any that might be used for certain military operations. While focused on this mission, the Information Assurance Directorate (IAD) had long been sought after to provide advice on security topics, and we held robust, productive, and mostly non-public relationships with a number of entities in the security and technology arenas as well as pure play businesses across a myriad of industries. IAD had the largest and, according to many, the most concentrated number of experts in security, from engineers, programmers, and cryptanalysts to

those with deep experience in the practical and implementable applications of security measures. IAD's engagements ran the gamut, from sharing in our mutual understanding of current or impending security challenges to partnerships that resulted in the development of security solutions to meet the challenges.

It was in this context that I was first exposed to corporate boards. During this time of significant cyber activity, it was not unusual for a company to contact senior NSA leadership to ask for help in understanding a particular threat. To the extent time and authorities permitted, we would provide our best judgement to help the board members understand cybersecurity at a basic level, understand how a particular event may be impacting their companies, and to help them navigate mitigation options.

WHAT ARE A BOARD'S DUTIES?

What was clear then is even clearer now. Corporate boards not only have fiduciary responsibilities to shareholders, but also a responsibility to be knowledgeable about key topics that could impact share performance. To meet these obligations, boards must be sufficiently informed, be provided with the right environment to ask, and get answers to, their questions. and be able to seek the advice of expert counsel when needed. The board environment must be conducive to learning and encourage dialog if board members are going to be best positioned to respond effectively in the event of a cyberattack.

Board members do not need to be deeply technical. But they do need to have lived experiences that help them understand cyber well enough to ask the right questions.

In these early engagements with boards on cyber incidents, there were a few prevailing themes. The first issue, of course, was: "What happened and why did it happen?" Knowing what happened was achievable, but knowing why was, and still is, a difficult climb. Stepping through the basics of cybersecurity, including threats, vulnerabilities, risks, and mitigations, was often sufficient preparation to begin the more complex discussions around motivations, threat actors, and impacts to the company.

Board members were eager to learn, but they were also frustrated with some of the technical complexities to which they had already been exposed. I realized that they needed clear explanations of cyber complexities in order to understand what could, and could not, be confirmed. It was during these sessions that I began to develop a personal passion for board service. I saw the need for having someone on a board who had a measure of depth in cybersecurity topics. That person, in my view, did not need to be deeply technical (I certainly was not), but did need to have lived experiences that positioned them to understand cybersecurity well enough to know the right questions to ask.

THE CYBERSECURITY CURRICULUM

What do boards need to know about cybersecurity to satisfy their fiduciary responsibilities? First, they need to understand what is at risk for their company in the event of a cyber incident. While this might seem to be a no-brainer, surprisingly it is not a topic they regularly consider. What are the company's crown jewels? Which threats to specific networks and/or data would have the gravest impact on the ability of the company to operate successfully? Areas that should be considered crucial to board knowledge and understanding include the following:

- **Insider Company Data:** Information regarding company strategies, competitors, financial plans, and schedules could impact a company's ability to remain competitive and deliver shareholder value.
- **Personally Identifiable Information:** Unauthorized access to PII held by the company could put others (e.g., customers or clients) at risk. This would include customer data that could be used for identity, for example a name, social security number, etc.
- **Intellectual Property:** Any cyber event that exposes IP could impact an entity's ability to continue to exist competitively, particularly if the IP is key to the company's business. Copyrighted and patented materials should be included in this list.
- **Competitive Data:** This includes contract bidding criteria, selection data, financial and legal data, and personnel files. Access to any of these could significantly impact a company's ability to perform, endanger its standing among peers, and affect its ability to hire and retain employees.
- **Reputation:** Threats to a company can upset and create uncertainty for shareholders, employees, and customers/clients. Their unease could translate into decisions to withdraw support (sell equity or switch to a competitor for products, services, employment, etc.). Reputational risk is not only very real, it's a compelling reason to act decisively and transparently in order to minimize impacts to trust.
- **Risk:** An understanding of the company's risk appetite is important to inform decisions that might need to be made in the event of a cyber event. Since managing risk is a prime responsibility of boards, including cyber risk in the topics they discuss is crucial to ensure the board is fully informed about the company's risk posture.
- **Education:** Can be achieved through periodic training sessions conducted either by inhouse or outside experts. Having an outside expert occasionally present to the board has the added benefit of giving them other perspectives and experiences.

The training should consist of the basics of cybersecurity (definitions and examples of threats, risks, and vulnerabilities and the relationships between them; explanation of mitigations versus responding after an attack has occurred; key legal, legislative, and regulatory rulings that apply to the company/business; and a history on any significant prior cyber events, particularly if they impacted the company). There are a multitude of opportunities for boards to be exposed to these basics, from books to online training opportunities for formal training provided by various credentialed organizations. What is important is that there is a clear, stated expectation that every board member will receive this basic exposure, and that periodic updates will be provided.

A company's incident response plan should specify criteria for board notification and any decisions that are their responsibility.

Next, a board needs to understand how the company protects networks and data. This includes the challenges it faces, the costs it incurs, and the areas that are not sufficiently funded. The information should be presented to the board on a regular (at least semi-annual) basis and should include a discussion about current threats—to the company, to others in the same business sector, to the broader business world. The board should know what the cybersecurity budget is and should be satisfied it is sufficient given the company's overall investment in technology and the risks inherent in the company's business. Evidence of a strong focus on cybersecurity includes:

- **Clear lines of authority for making decisions regarding technology and cybersecurity.** The company should have decision documents and processes that are documented and exercised regularly so that they are well-practiced in advance of an actual cyber event.
- **Sufficient budget to address current and emerging threats.** There are various metrics to determine what should be spent on cybersecurity. General industry standards suggest that 15% of the technology budget should be focused on security. This number should be modified based on several factors, including the size of the company and maturity of the business.
- **A knowledgeable, accountable, and proactive chief information security officer (CISO).** The CISO should meet with the board regularly and be viewed as the company expert on all things cybersecurity. This person should have demonstrated success in the field, an appropriate academic background, and should communicate regularly with CISO networks. This last point is especially important because CISOs often share threat information that later impacts their companies, providing an opportunity to prepare in advance of a cyber event. The CISO should be the point person for cybersecurity compliance issues, risk assessments, risk management, control decisions, service provider arrangements, penetration (and other) testing, security breaches or violations, management's responses, and recommended changes to the company's security programs.
- **A strong and sufficiently resourced IT/security team.** While having a strong CISO is important, equally important is having a strong team supporting the CISO. This team should have clearly defined roles and responsibilities. It should be the company's focal point for implementing security measures and responding to incidents.
- **A business continuity plan.** The board should receive regular (at least biannual) updates on data recovery, reconstitution, and storage plans. The ability to continue operations despite an attack can instill confidence in both customers/clients and employees.
- **A relationship with an expert cybersecurity firm that could be invoked as needed to assist with assessment, mitigation, and recovery.** Such expertise can assist with internal assessments, reconstitution, and any redundancy requirements.
- **An established personnel cybersecurity training and awareness plan.** This plan should not only include exercises on common exploits (e.g., phishing), but also inform personnel about new and emerging threats and their potential impacts on the company. It is well established that having such a plan and diligently exercising it creates a more aware workforce that is less likely to fall prey to an attacker's exploits.

THE BOARD'S ROLE IN INCIDENT RESPONSE

Given the current environment, a cyber event is likely to impact a company. Boards should be prepared for this by having a working knowledge of the company's plans should there be a cyberattack. One such plan is the incident response plan, which is a detailed document that defines how a company considers threats and how it will respond should there be an attack. This plan should not only define how the company will respond to an event, but also identify key individuals and their responsibilities, external resources available that the company could leverage, and should outline key aspects of a response to an incident. Having a company incident response plan is essential, and the board should be informed of the plan, ideally participating in periodic tabletop exercises that give the board an opportunity to see how the company intends to respond and to understand its own role.

An incident response plan should include guidance on how the company will respond, decision criteria for key operational continuity, recovery from an incident, communications, and engagement. This plan should specify the criteria for board notification, and any decisions that are their responsibility. Having this documentation ensures that the directors can fulfill their fiduciary duties, specifically the duty of care, in identifying how the company will operate if under attack, and what might constitute a decision to degrade or cease operations that could impact shareholder value. Making this decision is an important one and must be made with a fully informed view of impacts, outcomes, and long-term recovery needs. Recovery should be addressed from both from a technological as well as an operational perspective.

Knowing when to inform the board, how often to keep them informed, and when there is a decision that requires board approval is critical. Quite often, early in the life of an event, the information available is not verified. While this might cause management to delay notifying the board, management should consider at least informing the board of the fact of a validated event as early as possible. As cyber events progress and discovery results in learning about impacts not previously known or understood, it is best to have a board that is informed early and often so that they can be fully prepared to support management and fulfill their fiduciary responsibilities.

In the event of an incident, communications with the board regarding not only the incident, but any engagement with external legal or regulatory entities should be initiated and documented. Currently, all 50 states have data breach notification laws. Additionally, in July 2023 the SEC adopted rules governing incident disclosure requirements for public companies. Boards should be informed when an incident reaches the threshold that requires legal or regulatory notifications. This is important because, should there be any adverse responses to an incident, investigation could include interviews with board members. Keeping the board informed in a timely manner positions the directors to respond appropriately and exercise their fiduciary responsibilities of care and loyalty to the company and its stockholders.

THE BOTTOM LINE

There are other issues boards should consider as they focus on fiduciary responsibilities specific to cybersecurity. Should there be a board member designated as the "cyber expert"? Given the risks potentially impacted by a cyber event, should the CISO have a direct relationship with the board? Should the board be an approval authority for the company's security plan?

Once you start asking these kinds of questions, they keep flowing. And they suggest to me, at least, that boards have often been overlooked as players in this area. Should the board receive a periodic written report from the CISO regarding the state of security in the company? Do the company's insurance policies (property, casualty) cover business interruption losses caused by a network that is shut down due to a cyber event? Is the board's directors and officers (D&O) insurance sufficient? What are the terms and conditions for these policies? How should the board be involved in decisions regarding these policies? These are among the questions boards should be asking as they prepare to fulfill their fiduciary obligations.

Debora A. Plunkett, *a cybersecurity leader and educator, is a board member of CACI International, Nationwide Insurance, Mercury Systems, and BlueVoyant. She's also a Professor of Cybersecurity at the University of Maryland. She was the Director of Information Assurance at the NSA before she retired after 31 years and was a director on the National Security Council at the White House, where she focused on cybersecurity.*

AN OUTSIDER'S VIEW INSIDE CYBERSECURITY

DAVID HECHLER

Kyle McIntyre *has an interesting perch from which to view cybersecurity. He makes his living from it, but he's not really a part of it. His field is executive search. But since 2001, the recruiting company founded by his father in the late 1980s has specialized in this area. It started almost accidentally, but it quickly clicked. McIntyre Associates' first big cyber client was Foundstone (acquired by McAfee in 2004). The Foundstone engagement led to CrowdStrike, and from there it just kept going. Kyle joined the company in 2013 and began taking over from his father when CrowdStrike was prepping to go public. During the past decade he's watched both startups and enterprise clients handle the challenges of cybersecurity—as a business and as a security issue. He talked about the growing role of chief information security officers, and the distinction he makes between uppercase CISOs and lowercase cisos. He also offered insights into how companies might better integrate their boards into their cybersecurity strategies.*

David Hechler: In 2001, before you joined your father, Jeff McIntyre, the firm pivoted to specialize in cybersecurity. How did that happen?

KYLE MCINTYRE: An investor in Foundstone put him in touch with that company. And they called him up and asked, "McIntyre, what do you know about cyber?" Cybersecurity wasn't even a word back then. And he told them, "I don't know much about cyber." And they said, "We're going to ask you one more time, Jeff, what do you know about cyber?" And he said, "Listen, I'm your guy. I'm an expert." So they flew him out to meet the founder, a guy named George Kurtz, [who later co-founded CrowdStrike as well]. I think he realized pretty quickly that it was going to be a super growth opportunity.

DH: Indeed. I think your father was primarily working as a recruiter with startups, and they are prominent in your clientele. Do you remain focused on startups, or do you have larger clients as well?

KM: It's a bit of both. For the first four or five years in my career doing this, it was 100% focused on startups. Largely on CrowdStrike. But by the time CrowdStrike was coming close to an IPO [June 2019], we had

A lot of companies will hire a junior person and give them the CISO title just to check that box.

started doing work for some larger companies. I placed a CISO at Cisco Umbrella. That was probably the biggest company at the time that I had worked for. And then shortly after that, I was retained by United Technologies, which is now Raytheon, to help them build out their first-ever corporate-level product security center of excellence. Then we added Rockwell Collins, Otis Elevator, and Carrier Corporation. Now it's maybe 60% startups and the rest is a mix—both cybersecurity vendors and non-cybersecurity vendors.

DH: What have been some of the differences in the work?

KM: The CISO I placed at Cisco was in a cybersecurity vendor with Cisco Umbrella. So for the first time in my career, the focus was not on necessarily getting somebody who could help get to an exit [a sale or IPO], or help scale up revenue. Instead, for the first time, I was focused on finding nonredundant skill sets that would secure life-critical products. It was a straight line from my recruiting work to helping keep people safe in a physical sense. And since then, I've done some other things as well at larger companies, and some other midsize non-security companies. I've done CISOs for Commvault and work for a series D startup outside of security called FourKites. So I love working with startups, but I also really enjoy working with the larger companies as well. It's two different flavors for sure.

DH: Have the new SEC rules on cybersecurity changed the equation?

KM: The SEC regulations that we have today are still not as aggressive as you find in other countries. So we have work to do on the policies and regulations. But we have a lot more work to do in terms of companies out there coming up to speed. It doesn't seem like they're taking security that much more seriously in the wake of this. We did have a couple of newsworthy security events that I think are helping, and I've seen companies post CISO roles. I've even had conversations with companies about doing a CISO search in the last several months, but they were going to just promote somebody within or keep the person they have. I hope that they can get away with that and it doesn't bite them. But I think that companies are not diving headfirst into this new age of cybersecurity.

DH: I'll get back to CISOs, but talk to me about the newsworthy security events you mentioned.

KM: Well, the **MGM one** [reported in September] was pretty visible and kind of high profile. And I was struck by the number of security professionals and CISOs out there that were posting in support of MGM and the team. I don't know all the details of what happened there, but I think that one was visible enough where it got people to pay attention for a couple days or a week. We get these moments in time where the world, the enterprise, the private sector is paying attention to security for a minute. And then it takes a back burner again. I think it's going to continue to take these large financial consequences to push companies to pay attention.

DH: And when you say people are paying attention, among them are executives and board members at companies. It bubbles up when they see the headlines. And they often ask, "Could this be us? What are the risks?" So let me turn it around and ask, What kind of expertise in cybersecurity do you think executives and board members should have?

KM: Stepping outside of the cybersecurity vendor ecosystem, I look at companies' boards all the time. I like to stay in touch with who's doing what, but also what kind of profiles are on boards nowadays versus last year. And it's pretty rare to see a cybersecurity professional on a board. It's more common

to see a CEO that had an exit in security and is probably able to provide some insights. But is there a space for them to provide those insights? Whereas if you were to bring in a CISO with great business acumen onto the board, just by virtue of that person's background it almost forces there to be a space, right? But we have a long way to go. Boards have to be careful to not just check a box. It's the same conversation I have about CISOs, too. A lot of companies will hire a more junior person—nothing against that person—but hire a junior person and give them the CISO title just to check that box. And I would be mildly concerned that some boards might do the same thing.

DH: Do you think there's a problem that many startups have in their early days, when all they are focused on is the products they're trying to push out and they don't take time to focus on cybersecurity?

KM: Yeah. There's three pieces to this. Number one, you have the enterprise security. Number two, you have the product security, which often gets pushed to the side or it's an afterthought. And number three is revenue. Revenue is like oxygen for startups. And oftentimes security is viewed as purely a cost. And I guess there's another piece of this. I'll circle back and give you details on revenue in a minute. But the other piece is: Are we going to get hacked really? What are the chances that it's going to be us? You know, we're 100 people, we're not Cisco, we're not Amazon. Like, do we really need this? And maybe five years ago, you could roll those dice and the probability you're going to get breached or attacked would be pretty low. But today, it's a whole different ballgame. You have nontechnical bad actors that are able to do some real damage with tools that they just pull off the shelf, or credentials they can buy for a couple bucks on the dark web. So now it's a pretty high probability because bad actors are going for everybody and anybody they can get to.

DH: OK, let's come back to CISOs. You've talked about a lowercase ciso and an uppercase CISO. What do you mean?

KM: When I talk about a lowercase ciso versus an uppercase CISO, I'm not talking about the person's capabilities as much as I'm talking about the role that they're in and what they're allowed to do. I want to make that distinction. So I'm not talking about a junior person with a CISO title, although there is a lot of that out there. I'm really talking about how fully you are utilizing your CISO. For the uppercase you are using them as a thought leader, you are able to put them in front of customers, they do have board visibility, they can push back on your CEO and your board if something is important. You value their input, and you're paying them appropriately. The lowercase ciso role—I want to be careful here to not disenfranchise anybody—is basically the illusion of the uppercase role, but you have handcuffs on. You're not allowed to do what you would otherwise do, you're not fully utilized.

DH: So how do you help companies recruit the right person?

KM: I do everything I can on the front end of the search to make sure we don't end up with the wrong person, because you would hate to get somebody who's phenomenal and then have them quit in a year, right? It's not good for anybody. And so on the front end of a search discussion, even before I'm retained, I always like to define the parameters. Like, "Hey, potential client, let me have this uppercase, lowercase CISO conversation with you, and you tell me which one you think you want. And then we'll talk about which one you can actually afford."

So circling back to the revenue piece—and this is a conversation I always love to have on the front end of a CISO search—what do you guys really think you need? And here's what a real CISO is going to bring to the table. And oftentimes, as I said, security is viewed as a cost center. It doesn't have to be purely a cost center. It's going to cost you money, but if you hire the right person who can speak with customers, it can also offer you a competitive advantage. And if you hire the right person who can be a thought leader in security, go to the security conferences, speak at Black Hat, then you have another way that the CISO or the security leader is bringing value to your organization. And it's not just in the form of

keeping you safe. It's not just in the form of helping you drive more revenue when those opportunities arise to connect your CISO with a potential client. It's also helping build your brand, in terms of: This is a company that is socially responsible, that cares about security and keeping the world safe.

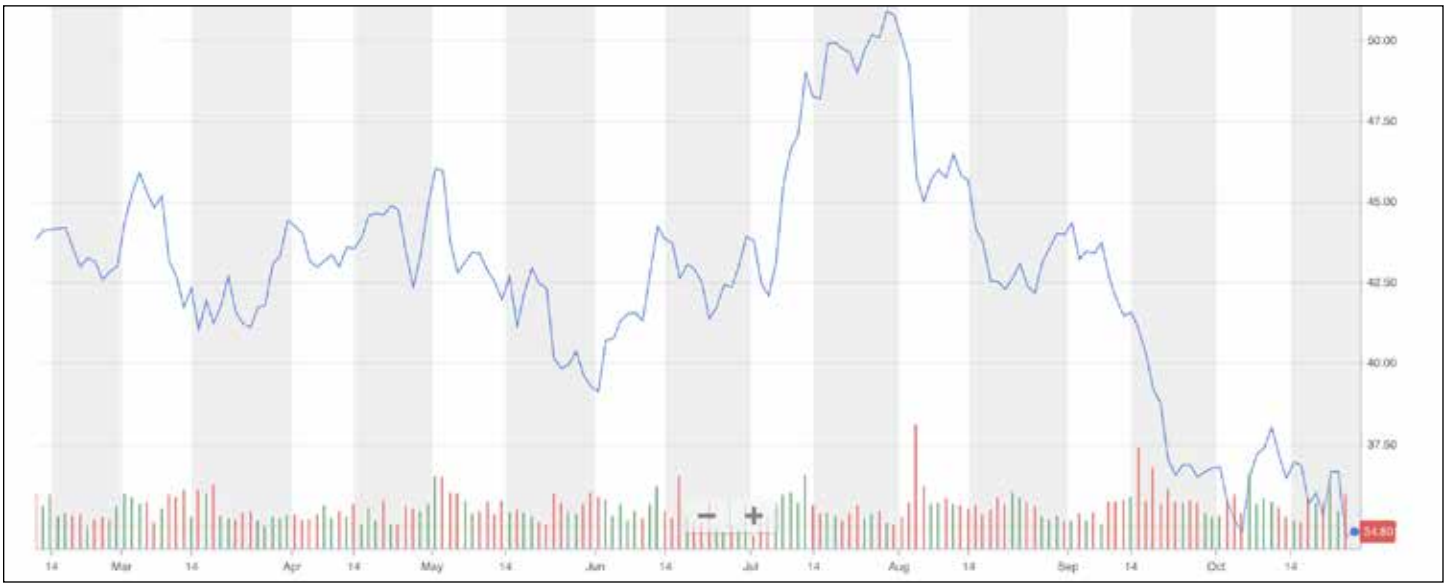
DH: The prosecution and conviction of Joe Sullivan, the former chief security officer at Uber, has drawn enormous attention. How has it affected CISOs and the CISO marketplace?

KM: I think that the conversation versus what's actually happening are two different things. The conversation I hear a lot is that the CISO role is more risky now. There's a precedent set. But it's a lot of talk. I'm not seeing a lot of change in terms of what the CISO role looks like and who's willing to explore new roles. I'm still having conversations with the same kinds of people about the same kinds of roles. But there is this subterranean tension around what's going to happen next. I think a lot of CISOs and security professionals are just burned out. So many of them get disrespected in their company, in their team, in their industry.

DH: Is it fair to say that for a long time when there was a big breach at a big company that had a CISO in place, and somebody needed to be blamed, the easiest, most expeditious thing was to fire the CISO? And everybody was kind of used to that, although it certainly was a burden on CISOs to know that they were sitting in a hot seat that could be an empty seat pretty soon. But the idea that they could end up sitting in a prison was not something they had contemplated. Is that a fair assessment?

KM: Yeah. I think it blew everybody's mind. And I think a lot of CISOs were not as—like it was shocking but not surprising. And, by the way, on that note of swapping out your CISO every year or two, I mean, that might work once or twice. But how good do you look as a company when you've had four different security leaders in five years or something? But yeah, I think it was a big shock to everybody. And I hope it's not a precedent that sticks. The CISO shouldn't be an army of one. They're part of the management team. And they have a team, and they have other stakeholders, and they have people influencing their decision-making, and what they are and are not allowed to do. And the more visible the CISO can be on a regular basis to the board, the better in terms of helping protect them. So that when something happens, it's not as much of a surprise. They can say, "Well, I've been trying to tell you guys, we need to buy this product, we need to close this gap." Whatever it is. And I think there's been a lot of gatekeeping between the CISO and the board.

And on that note, I'm not sure that companies' stocks are feeling the consequences of these breaches. At the companies themselves, it's a whole different story. I'm sure at MGM everybody's running around with their hair on fire. I haven't looked at a **stock chart** for that one. But I do think that the



YAHOO/FINANCE

A six-month stock chart for MGM Resorts International shows that the company's stock price dropped after a major breach was reported in September.

consequences—they're not hitting their wallet the way I thought they would. That is one of the reasons we're not paying enough attention even now. It all comes back to money. You follow the dollars.

DH: You haven't done any recruiting of board members yet, but you said that it's just a matter of time. What kind of role do you think boards ought to be playing in cybersecurity? And what level of knowledge and experience would it be useful for them to have as a group? You talked about the idea of a CISO on the board. How important might that be?

KM: There's so many boards out there that are completely uninitiated in terms of thinking about cybersecurity beyond the Norton Antivirus that's on their laptop. At the board level, it's got to be a person who can speak that language, who can know when to push back and know when to stop somebody and try to correct them. It has to start with the person being a great communicator and being able to exercise restraint.

An adviser should be willing to meet the board where they're at. Don't start talking bits and bytes if what you really need to be doing is talking about dollars and cents.

DH: Someone on the board or someone who's communicating with the board?

KM: Even an adviser to the board, even your CISO. Even if they're not on the board, even if they don't have regular board interactions. When you do call them to step up to the plate and talk to your board, you want somebody who's going to make you look good, right? But also can be effective and change hearts and minds—if that's what you need. And again, a lot of these board members haven't had to think about this. It hasn't been impacting revenue, it hasn't impacted their exits and things like that. I think this person, the adviser, if it's a CISO that's on the board, has to be willing to meet them where they're at. If we need to start with the super big picture and slowly zoom in more and more, then that's what they need to do. Don't start talking bits and bytes if what you really need to be doing is talking about dollars and cents.

"It's never too late to purchase our SEC cyber reporting platform."

DH: Do you think there ought to be some regular communication established in a company that doesn't have board members with experience and expertise in cybersecurity, or a cybersecurity security committee that's part of the board? Do you think they ought to connect with the CISO or outside experts to initiate a regular education program?

KM: I think in a perfect world, we have that. I don't know how willing busy board members will be to do that on a regular basis. But if you're lucky enough to have a great security leader available to you, if it's somebody inside your company or somebody who is willing to lend their insights, and you can do it on a quarterly basis or three times a year and take advantage of current events—like here's this MGM event and here's how it applies to us. I think that sometimes, especially for business people who are not technical, you need to tie it to something that hits home. And oftentimes that's the money.

INTERVIEWS

AN INTERVIEW WITH DAVID CHARTIER
CEO, ARCTIC SECURITY

ENHANCING CYBERSECURITY RESILIENCE AND COMPLIANCE

In a recent discussion with TAG, we discussed Arctic Security's dedication to providing advanced warning of cyber threats and expertise in threat intelligence and proactive defense strategies. Join us as we delve into the methods that drive Arctic Security's mission to equip organizations with early insights into looming cyber threats, shedding light on their practical approach to evolving digital risks.

TAG: How does Arctic Security's threat intelligence platform adapt to the specific cybersecurity needs and challenges of different industries?

ARCTIC SECURITY: While industries differ from their operational business perspective, they all share much of the same core IT infrastructure. Criminals find industry-specific vulnerabilities to exploit and use, which requires additional work and reduces the target pool. Ensuring the core infrastructure is secure is essential for any company's resiliency.

From malware infections to known security vulnerabilities, we cover an extensive list of precursors to ransomware. We help financial industry clients detect ransomware in the very early stages, allowing them to isolate systems and prevent a ransom demand against the organization. We also work with our MSSP partners servicing the financial sector clients to offer the best possible coverage.

In healthcare, clients use our triaged vulnerability data to assist their understaffed IT teams in addressing urgent security concerns and preventing breaches. The internal staff often faces uncertainty about the order of priority for addressing issues, leading to prolonged risks. With our external perspective, we assist them in prioritizing the most high-risk, easily exploitable problems.

We process 20 million daily incidents, filter them for each customer, and alert them to fix specific issues. This approach saves time and costs a fraction of what companies would spend if they performed it themselves. Early warning involves detecting and addressing issues before they cause harm to organizations.

We help financial industry clients detect ransomware in the very early stages, allowing them to isolate systems and prevent a ransom demand against the organization.

TAG: Can you provide examples of organizations successfully integrating Arctic Security's threat intelligence into their security stack?

ARCTIC SECURITY: A medium-sized university initially implemented Arctic EWS to safeguard its infrastructure, revealing numerous compromised machines in its network. They resolved the issues, investigated the cause, and discovered that their newly installed firewalls lacked proper setup and maintenance. Arctic EWS aided their realization of the problem and enabled them to enhance their security posture.

Some MSSP partners engage post-breach and conduct root-cause analysis. They've found, by reviewing historical Arctic EWS data, that vulnerabilities leading to breaches were exposed and exploitable for months beforehand. Early warning is a vital foundation for preventing security incidents. Consequently, many of their incident response clients subsequently subscribe to Arctic EWS.

These results emphasize the need for continuous external monitoring and prompt security problem resolution, as criminals will exploit exposed pathways to the organization sooner or later.

TAG: How does Arctic Security ensure the timely and accurate delivery of threat intelligence to its customers?

ARCTIC SECURITY: We originally developed our platform to stream real-time data for our nation/state customers serving large numbers of organizations. Other vendors who initially focused on individual enterprise customers typically lack this unique perspective. Accuracy is one of the guiding core values of our business, especially for large-scale operations.

Arctic EWS continuously monitors and updates the attack surface, generating a comprehensive list of issues. We report real issues that impact the company and its vendors. Early warning relies on accuracy as every false positive consumes our clients' time and money — resources they can't afford to waste.

As the threat landscape evolves, we save our customers' time by incorporating new data sources to expand coverage against emerging threats. Our partnership with national cybersecurity centers also enhances our understanding of reliable threat data sources, aligning with our shared mission to bolster national infrastructure resilience against cyber threats.

Arctic Security provides data to national cybersecurity authorities to monitor security issues in their region. We leverage our expertise in identifying known security vulnerabilities, offering it as a data service for those building their own context-specific early warning services.

TAG: What mechanisms does Arctic Security offer to facilitate collaboration among security teams and the sharing of threat intelligence?

ARCTIC SECURITY: EWS's comprehensive issue categorization allows the dissemination of information to the correct group/team in the enterprise, which, in turn, facilitates issue remediation. At the client's organization, each category of cybersecurity issues we deliver to our subscribers caters to a specific audience. Additionally, Arctic EWS offers a monthly overview report for stakeholders and boards, enabling them to assess the performance of their security programs and engage constructively with the security staff.

Our national cybersecurity center customers utilize our platform's interconnectivity APIs to exchange and distribute information, enhancing their early warning services. This process aids in delivering more information to victim companies, enabling them to address issues promptly.

TAG: How does Arctic Security assist organizations in complying with regulatory requirements related to threat intelligence sharing and reporting?

ARCTIC SECURITY: Many of our European customers are preparing to meet the requirements of the NIS2 directive that mandates external monitoring of their infrastructure and reporting of breaches to the authorities. With one year to prepare, many are looking for practical solutions to handle the upcoming changes quickly.

Our real-time monitoring capability has helped them meet many of those requirements well before the 2024 enforcement date for the directive. They can fix security vulnerabilities ahead of time and stay on top of their attack surface to avoid having to report a breach through the official channels in the first place.

AN INTERVIEW WITH DEBBIE GORDON
FOUNDER AND CEO, CLOUD RANGE

COMPREHENSIVE CYBERSECURITY TRAINING SOLUTIONS AND UNIQUE FLEXRANGE PROGRAMS

In an interview conducted by the TAG Analysts, Cloud Range's expertise in SOC (Security Operations Center) training takes center stage. As the cybersecurity landscape continues to evolve, Cloud Range's pragmatic approach to enhancing organizations' cyber resilience has garnered attention across the SOC community. This conversation addresses the core methodologies underpinning Cloud Range's mission to prepare organizations for managing and mitigating cyber threats through comprehensive training programs.

TAG: Can you explain how Cloud Range's FlexRange Programs contribute to the preparedness of security teams and what makes them unique in the industry?

CLOUD RANGE: With an acute shortage of cybersecurity professionals worldwide, it's challenging for organizations to find, hire, and retain experienced, battle-ready cyber defenders. Security personnel are the last line of defense against cyberattacks, but traditional education and certifications are not enough, and on-the-job training is not an option.

It's critical that security teams regularly train and practice detecting and responding to cyber threats, understand attack vectors and tactics, test their playbooks, and, for IT and OT teams, speak the same language and understand how systems integrate.

Cloud Range fills the experience and skills gap with FlexRange™ Cyber Range and Simulation Training, an ongoing live-fire IT and OT/industrial incident response simulation exercises program. Just as pilots must train in a flight simulator, FlexRange enables security teams to practice defense against real-world cyberattacks, maximize toolsets, and improve operational efficiency. Security leaders and teams are drawn to Cloud Range's FlexRange program because it solves a universal problem with a quality readiness solution that strengthens resilience, shows measurable results, and reduces the organization's risk.

Just as pilots must train in a flight simulator, FlexRange enables security teams to practice defense against real-world cyberattacks, maximize toolsets, and improve operational efficiency.

FlexRange is unique in the industry with customizable, cloud-based virtual ranges and the only live-fire OT/ICS cyber range for team training. The safe enterprise network environments include application servers, email servers, OT components, switches, routers, traffic, alerts, and integrated industry-leading security products such as SIEMs, firewalls, IDSs, endpoint security systems, analysis tools, and more. Plus, Cloud Range regularly develops new IT and OT cyberattack scenarios based on threat intelligence.

Cloud Range's full-service model simplifies cyber training with live instructors, customized program design, range administration, and program management to help teams achieve their goals. An integrated learning management system tracks progress, considering NICE Framework KSAs, MITRE ATT&CK TTPs, industry regulations, job requirements, technical skills, soft skills, and detection time. This unique, tailored approach is unmatched in today's market.

TAG: Can you elaborate on the types of team simulation exercises offered by Cloud Range?

CLOUD RANGE: Unlike other "team" training types that are simply a group of people working on solo courses in parallel, Cloud Range's simulation exercises ensure each person works as part of a true team, each with a different role and contributing to the team's success.

Examples of Cloud Range's dynamic attack scenarios include ransomware, phishing, DNS tunneling, website defacement, OT/ICS attacks, DDOS attacks, supply chain attacks, and more.

Multiple learning formats have thousands of simulation options, including red, blue, red vs. blue, and purple team training exercises, capture-the-flag events, skill development labs, challenge labs, and next-generation tabletop exercises.

TAG: How does Cloud Range tailor its FlexRange Programs to meet the specific needs of different organizations?

CLOUD RANGE: We tailor our FlexRange programs to each organization's goals and team members' experience levels. Within the range, customization options include the network environment, architecture, tools, attack type, amount of traffic, complexity level, and more. For OT/ICS environments, the range includes virtualized HMIs, PLCs, monitoring tools, and hardware-in-the-loop (HIL) capabilities, enabling the range to directly connect to a customer's live, physical lab environment.

Cloud Range's tech team is on hand to create new scenarios, incorporate additional tools, and provide other customizations as needed.

Plus, in addition to team training, each team member receives individual coaching. Customized learning plans are generated in Cloud Range's Performance Portal is based on each person's goals, roles, assessments, progress, and organizational criteria. Doing this ensures every cyber practitioner regularly grows in their field and careers while reducing the burden on leadership to manage this for their teams.

TAG: What role do soft skills, such as communication and collaboration, play in Cloud Range's training programs, and how do they contribute to cyber readiness?

CLOUD RANGE: Besides improving the SOC's technical ability to respond to a significant attack, Cloud Range's training programs help teams enhance critical thinking, problem-solving, communication, judgment, and teamwork. We include these soft skills in the evaluation and executive debrief that Cloud Range provides to security leaders.

Soft skills are vital in cybersecurity. Effective teamwork and communication under pressure lead to quicker incident resolution, timely information sharing, and better articulation of risk factors, fostering productive discussions within the team, the board, executives, legal, partners, and customers. FlexRange training enhances security team collaboration, threat management, and professional growth for better preparedness.

TAG: Can you explain the significance of OT (Operational Technology) training scenarios and how they help address the rising threats to critical infrastructure?

CLOUD RANGE: The digital convergence of OT and IT has increased the number of cyberattacks that affect OT/ICS environments. However, OT and IT teams are often unaware of each other's techniques, objectives, or protocols. They require unique training to ensure they can speak the same language and overcome the distinctive OT/ICS threats and challenges they face.

Cloud Range offers dynamic, live-fire OT/ICS, OT/IoT, and IT/OT incident response and security operations training for various industrial sectors, including energy, water systems, nuclear, transportation, and buildings/facilities. This innovative solution enhances security, team resilience, and operational efficiency and promotes IT and OT team collaboration to mitigate organizational friction and complexity.

Our OT/ICS scenarios provide practical training for responding to real cyberattacks, following the MITRE ATT&CK Frameworks. This immersive, live-fire, cloud-based cyber range platform equips teams with the necessary expertise, judgment, skills, and muscle memory to safeguard data and human lives.

AN INTERVIEW WITH MATAN OR-EL
CO-FOUNDER AND CEO, PANORAYS

ADAPTIVE APPROACHES TO THIRD-PARTY RISK MANAGEMENT AND COMPLIANCE

TAG analysts recently caught up with Panorays to learn more about their automated third-party risk management proficiency. As businesses increasingly rely on a network of external vendors and partners, Panorays' practical approach to assessing and mitigating third-party risks has become super important to the industry.

This conversation covers Panorays' mission to streamline and enhance third-party risk management, offering insights into their pragmatic strategies for navigating the complex landscape of vendor-related vulnerabilities and security concerns.

TAG: How does Panorays' third-party security management platform adapt to different industries' specific compliance and risk management requirements, such as healthcare or financial services?

PANORAYS: Panorays excels at adapting its third-party security management platform to diverse industry cyber security compliance and risk management needs. In healthcare, for example, where safeguarding sensitive patient information is paramount, Panorays aligns its security controls with healthcare compliance standards like the Health Insurance Portability and Accountability Act (HIPAA), ensuring third-party vendors adhere to strict data protection and privacy regulations.

Another example is compliance with the Sarbanes-Oxley Act (SOX), which is crucial in the financial services sector due to its stringent regulations ensuring transparency, accurate reporting, and corporate accountability for public companies in the United States. Panorays' platform integrates specialized security measures and compliance checks to ensure third-party vendors comply with financial regulations, including data encryption, transaction security, and overall information protection. This tailored approach allows organizations to effectively manage third-party security, mitigate risks, and uphold compliance standards specific to their industry.

Real-time monitoring tools are indispensable across various industries for overseeing vendors' and third-party activities while promptly identifying deviations from established security protocols. These tools enable organizations to

Panorays maintains up-to-date awareness of emerging cyber threats and vulnerabilities through continuous monitoring, industry research, threat intelligence feeds, and collaboration with cybersecurity experts.

take proactive measures in risk management by continuously monitoring real-time data access, network traffic, and system utilization. Detecting odd patterns or potential breaches allows organizations to act fast, reducing the risk of unauthorized access or data breaches. This proactive approach improves the organization's security and helps it respond better to changing cyber threats, protecting sensitive data.

TAG: Can you share examples of organizations successfully improving their third-party risk posture and compliance standing using Panorays' solutions?

PANORAYS: Many organizations have successfully improved their third-party risk posture and compliance standing by leveraging Panorays' solutions. Examples include Arvest Bank, UBS, Payoneer, Sapiens, and many others. These businesses utilized Panorays to strengthen potential vulnerabilities within their cybersecurity infrastructure.

Customers choose Panorays for its dynamic automated questionnaires, external digital footprint assessments, and comprehensive risk ratings that consider the business relationship context. Our customers benefit from Panorays as it allows them to streamline their third-party security evaluation process and gain a holistic view of vendor and third-party security, which in turn helps reduce manual efforts.

The automation and comprehensive insights provided by Panorays significantly contribute to our customers' ability to manage third-party security risks efficiently. This enhances their security posture and facilitates feedback with third parties for accurate remediation tasks, allowing efficient risk mitigation.

These companies took a proactive approach that helped them identify and remediate cybersecurity gaps, ultimately strengthening their overall security.

TAG: How does Panorays stay current with evolving cyber threats and vulnerabilities to provide timely risk assessments and customer recommendations?

PANORAYS: Panorays maintains up-to-date awareness of emerging cyber threats and vulnerabilities through continuous monitoring, industry research, threat intelligence feeds, and collaboration with cybersecurity experts. We analyze trends, assess potential risks, and incorporate the latest threat information into our platform. We cross-match this data with each customer's supply chain, allowing us to provide tailored, timely, and accurate risk assessments and recommendations to mitigate and manage risks. The dynamic approach ensures that Panorays remains at the forefront of cybersecurity, addressing evolving threats to enhance their customers' security posture.

TAG: Can you elaborate on the integration capabilities that Panorays offers to connect with various vendor risk assessment tools and enhance the overall security ecosystem?

PANORAYS: Panorays offers versatile integration capabilities to seamlessly connect with various vendor risk assessment tools, enhancing the overall security ecosystem. Panorays enables automated data exchange and communication with diverse tools through API integrations, streamlining the risk evaluation process. This includes integrating third-party risk platforms and facilitating comprehensive risk management by incorporating Panorays' assessment data.

The platform also supports automated sharing of crucial risk assessment data and seamless workflow integration, making risk assessment an integral part of daily operations. The integration is scalable, flexible, and provides real-time updates, ensuring organizations can promptly adapt to their specific needs and stay updated on risk statuses. These integrations empower organizations to fortify their security by incorporating efficient risk assessment seamlessly into their existing frameworks.

TAG: What role does automation play in Panorays' platform, and how does it streamline the vendor risk assessment process while ensuring accuracy?

PANORAYS: Automation is a core component of Panorays' platform, streamlining vendor risk assessments for accuracy and efficiency. The platform automates data collection, risk analysis, and reporting, reducing manual effort and human errors. Automated workflows gather and process information from diverse sources, such as external attack surface assessments and security questionnaires, accelerating the assessment process and providing real-time insights into vendors' security postures.

Consistency is ensured through standardized criteria and risk metrics applied consistently across all vendors, enabling fair comparisons and informed decision-making. Automated alerts and notifications keep stakeholders updated on critical changes, bolstering responsiveness to emerging threats promptly. By leveraging automation, Panorays optimizes the vendor risk assessment lifecycle, allowing organizations to manage and mitigate risks effectively, precisely, and quickly.

AN INTERVIEW WITH GREG ENRIQUEZ
CEO, REDSEAL

ENHANCING NETWORK SECURITY THROUGH CONTEXTUAL INSIGHTS AND PREDICTIVE MODELING

In a recent interview conducted by TAG, RedSeal's proficiency in network exposure analytics for cybersecurity and compliance takes the spotlight. In an era where network vulnerabilities not only persist but pose increasingly significant threats, RedSeal's pragmatic approach to closing defensive gaps has proven to be the missing link in many organizations' security strategies."

The conversation summarized below explores the core methodologies that underpin RedSeal's goal to provide comprehensive network insights through modeling and analysis, offering practical strategies for addressing the evolving challenges of network security and compliance in the modern digital landscape.

TAG: What sets RedSeal's cyber analytics platform apart in visualizing and understanding an organization's attack surface, especially for complex, multi-cloud, and hybrid environments?

REDSEAL: It's all about context. RedSeal goes beyond merely identifying vulnerabilities; it puts them in the context of your network topology and security policies. RedSeal integrates with many different security tools and technologies, both on-premises and in the cloud, providing an accurate and comprehensive visualization of your network. This integration helps you truly know what you have, how it's connected, and what's at risk. That includes identifying which paths an attacker might take to move laterally within the network.

RedSeal builds a digital twin of your network, simulates attacks, runs compliance checks, and prioritizes the risks based on that contextual understanding. Understanding the vulnerabilities exposed to the internet and the exploitable misconfigurations that can affect critical systems and data is vital. This understanding proves indispensable for prioritizing and accelerating remediation efforts within intricate, hybrid environments, demanding more intelligent and swift collaboration among teams.

TAG: Can you provide examples of organizations that have improved network security and resilience by leveraging RedSeal's platform?

REDSEAL: One of our customers previously spent $5 million annually on manual assessments

RedSeal helps organizations be more proactive about cybersecurity and compliance.

of their extensive global network infrastructure, ranging from small-scale setups to enterprise-grade architectures. A team of over 15 people meticulously documented network gear and configurations and performed vulnerability checks, but this manual process proved error-prone, time-intensive, and unsustainable. With RedSeal, they now automatically identify and assess vulnerabilities while continuously comparing network devices to industry standards, STIG checks, and CIS benchmarks. The results include significant cost savings and valuable, accurate data on their security and risk posture.

Another great example is a large health system in Pennsylvania with 20,000 clinicians caring for hundreds of thousands of patients annually. They experienced tremendous network growth and needed visibility of over 150,000 medical devices connected to IoMT (Internet of Medical Things) to prioritize risk and determine where to spend time and resources. With RedSeal, they now have a complete visualization across their complex, hybrid network. With the RedSeal/Medigate integration, the organization is discovering, assessing, and prioritizing cybersecurity risk and achieving compliance using the MITRE ATT&CK framework.

TAG: How does RedSeal adapt to organizational network and security infrastructure changes, ensuring ongoing accuracy and relevance in risk assessments?

REDSEAL: Our product continuously monitors an organization's hybrid network, conducting scans and collecting data from the network, network devices, and security policies. When users introduce new devices, modify configurations, or introduce vulnerabilities, RedSeal remains aware of these events and issues alerts and notifications when it detects alterations in the network or security configurations. These alerts promptly inform users about potential risks or deviations from the intended state and empower them to analyze changes in the network and infrastructure, enabling them to prioritize remediation.

TAG: Can you share insights into the integration capabilities RedSeal offers to enhance collaboration with other security tools and technologies?

REDSEAL: We offer seamless integration with over 125 security tools and technologies, reducing the time and resources needed for a complete view of on-prem and cloud networks. RedSeal integrates with everything from SDN/Clouds, service chains, and IOT/OT applications to routers, switches, firewalls, encryptors, vulnerability managers, SD-Wans, and more. For a complete list, check out the integration guide on our website. We invest heavily in building these integrations and making them easy to implement. Our integration capabilities validate the efficacy of vulnerability scans and foster collaboration among different security and network teams. This approach ensures the timely

identification and mitigation of security weaknesses, contributing to a more resilient and secure network environment.

TAG: What role does predictive modeling and simulation play in RedSeal's platform, and how does it assist organizations in proactively identifying and addressing security weaknesses?

REDSEAL: Predictive modeling and simulation play a crucial role in RedSeal's platform by helping organizations be more proactive about cybersecurity and compliance.

RedSeal uses predictive modeling to simulate attack paths within a network, assuming attackers seek the most efficient route from compromise to high-value targets. This helps organizations grasp vulnerability exploitation and assess the threat landscape. Teams can identify network weak points and proactively strengthen controls, patch vulnerabilities, or adjust access policies before real attackers strike.

Predictive modeling prioritizes vulnerabilities by their potential impact. It identifies vulnerabilities and assesses their likelihood of exploitation. High-risk attack path components or those affecting critical assets receive top priority, enabling security teams to focus on the most vital areas.

RedSeal also uses predictive modeling to assess and quantify the risks associated with different vulnerabilities, attack paths, and network configurations. This enables organizations to make informed decisions about where to allocate resources for mitigation and risk reduction.

RedSeal's "What if?" simulation capabilities allow organizations to assess the impact of changes to network configurations, firewall rules, or security policies before implementing them. This proactive approach helps prevent misconfigurations or policy changes that could inadvertently introduce security weaknesses.

We use predictive modeling and simulation to validate compliance with industry standards, regulations, and best practices. RedSeal assesses network configurations against predefined benchmarks, highlighting areas needing improvement for proactive compliance. Predictive modeling is an ongoing process of continuous monitoring. RedSeal helps organizations adapt to threats and network changes, swiftly addressing security weaknesses.

AN INTERVIEW WITH GUY BEJERANO
CEO & CO-FOUNDER, SAFEBREACH

REVOLUTIONIZING CYBERSECURITY RESILIENCE WITH SIMULATION EXPERTISE

During a recent interview with TAG, the focus shifted to SafeBreach's breach and attack simulation expertise. SafeBreach's practical approach to actively testing and strengthening cybersecurity defenses has garnered attention in an ever-changing threat landscape.

This discussion explores the fundamental methodologies that underpin SafeBreach's objective of emulating real-world cyberattacks, providing valuable insights into their practical strategies for bolstering cybersecurity resilience through vulnerability identification and response mechanism optimization.

TAG: How does SafeBreach's breach and attack simulation platform assist organizations in proactively identifying and addressing security weaknesses and vulnerabilities?

SAFEBREACH: The SafeBreach platform leverages the tactics, techniques, and procedures (TTPs) that malicious actors use to simulate real attack scenarios continuously. As a result, organizations can quickly understand whether their security controls effectively detect, prevent, or mitigate attacks across the entire cyber kill chain. This proactive approach continuously validates cloud and on-prem security controls, tests security posture, discovers and mitigates critical gaps before adversaries can exploit them, and prioritizes and automates remediation.

SafeBreach also impacts an organization's ability to understand and report on risk, ensure alignment with frameworks like NIST and MITRE ATT&CK, and support compliance by proactively identifying and remediating vulnerabilities before they lead to regulatory violations. Finally, the platform can improve overall SOC efficacy by testing current detection capabilities and incident response playbooks, which helps to prioritize security program spend.

TAG: Can you share success stories of organizations that have improved their cybersecurity posture and incident response capabilities?

SAFEBREACH: We work with some of the world's largest enterprises—like Experian, Union Pacific Railroad, Humana, PayPal, Olin, Paychex, Regeneron, and Carlsberg—across diverse sectors that include financial services, healthcare, life

The SafeBreach platform leverages the tactics, techniques, and procedures (TTPs) that malicious actors use to simulate real attack scenarios continuously.

sciences, public utilities, manufacturing, and transportation. The SafeBreach platform supports various use cases, including security control validation; threat, cloud security, and compliance assessments; portfolio rationalization, risk-based vulnerability management, security team training, and more.

In our first example, the Carlsberg Group, a global company operating in 150 countries, faced the challenge of safeguarding its production lines from evolving cyber threats. To go beyond the limited security tools like penetration testing, red teaming, and vulnerability scanners, Carlsberg adopted the SafeBreach BAS platform, which enabled ongoing, precise replication of real-world attack scenarios, continuous security control validation, uncovered previously undetected gaps and vulnerabilities, revealed new attack vectors, and established a strong security foundation. This foundation supported future security solution testing, streamlined Mergers and Acquisitions (M&A) processes, and met evolving business needs.

Our second example is the leading Financial Services Institution (FSI), which faced a significant internal alert chain issue despite having a mature security program in place. Notifications often weren't delivered to incident responders or were delayed due to the complex pipeline of technologies, which created a critical gap for malicious actors to exploit. To utilize automated health checks for incident response tools and processes, the FSI implemented SafeBreach's BAS platform to simulate realistic attack scenarios and validate the efficacy of its security tools, alert and detection systems, and incident response workflows.

Consequently, the FSI validated its security tools with tailored attack scenarios mirroring real-world threats. They proactively identified alerting issues, discrepancies, and potential escalations while achieving comprehensive end-to-end visibility through a closed-loop approach encompassing alerts, simulated response actions, and outcome verification. These measures reinstated the FSI's confidence in detecting and responding to threats.

TAG: How does SafeBreach adapt to the evolving threat landscape, ensuring its simulations cover the latest attack techniques and tactics?

SAFEBREACH: SafeBreach maintains a dedicated threat research team that actively monitors the hacker underground, utilizes intelligence feeds, and conducts research to ensure our Hacker's Playbook remains the world's largest and most up-to-date collection of exploits and known attack types. Our playbook includes 30,000+ breach methods for continuous security control testing. We are the only BAS vendor with a 24-hour service-level agreement (SLA) to incorporate new attacks based on **critical US-CERT and FBI Flash alerts.** Our research team is recognized for their real-world experience and industry contributions,

frequently speaking at global cybersecurity events. Their work has appeared in TechCrunch, Dark Reading, and SC Magazine, with four presentations at Black Hat and DEFCON this year alone.

TAG: Can you provide insights into the reporting and analytics capabilities of SafeBreach's platform?

SAFEBREACH: The SafeBreach platform enables organizations to analyze attack simulation results in real time, assessing the performance and effectiveness of deployed security controls. Results are categorized, including MITRE ATT&CK® framework data, known attacks, and threat groups. The platform visualizes attack paths and supports the exploration of alternative mitigation strategies through customizable dashboards. SafeBreach reports include a single exposure score, allowing security teams to measure their baseline, track progress, and align security program reporting, KPIs, and investments with business goals.

TAG: What support and guidance does SafeBreach offer organizations to translate simulation results into actionable security improvements?

SAFEBREACH: We view BAS as a comprehensive program, not just a standalone product, and prioritize service and support to ensure our customers' success. This includes our SafeBreach-as-a-Service (SBaaS) program, where our award-winning Customer Success Team collaborates with customers to implement the SafeBreach platform. They leverage the platform's features to integrate simulation results with existing business systems and workflows. Additionally, our world-renowned research team provides research and threat modeling support.

We also provide various resources customers can leverage, including comprehensive user manuals, support documentation, and supplemental content. We have an online portal where customers can access the SafeBreach Academy for a personalized onboarding experience at the user's own pace. We also offer the SafeBreach Community, where customers can find FAQs, submit questions to SafeBreach support experts, and engage with each other.

Finally, we host our **Validate Summit**, a recurring, in-person event that connects our customers and security experts to discuss challenges, best practices, and critical considerations for building a proactive security program. This event features insightful panels and hands-on sessions designed to help customers network with their peers, learn best practices from one another, and hear how other enterprises are leveraging BAS to enhance their cyber resilience.

AN INTERVIEW WITH AUSTIN GADIENT
CTO & CO-FOUNDER, VALI CYBER

EXPLORING ADVANCED LINUX SECURITY AND MULTI-CLOUD BENCHMARKING SOLUTIONS

We recently interviewed Austin Gadient, Vali Cyber's CTO and Co-founder, to discuss how their ZeroLock™ platform secures Linux environments and detects malicious activities. We cover its unique features like behavioral analysis, lockdown rules, seamless integration, and GDPR and CCPA compliance efforts. Read on for insights into Vali Cyber's innovative solutions and commitment to enhancing cybersecurity and compliance.

TAG: How does Vali Cyber's ZeroLock™ platform secure Linux environments and detect/stop malicious activity?

VALI CYBER: The ZeroLock platform employs advanced techniques to ensure the security of Linux environments and effectively detects and halts various forms of malicious activity, such as ransomware, cryptojacking, attacks by malicious actors with stolen credentials, and exploits targeting known vulnerabilities.

ZeroLock utilizes behavioral analysis to identify suspicious activities and anomalies within Linux environments. Its agent autonomously monitors processes, system calls, network traffic, and file access patterns to detect malicious. It responds in real time, stopping the attack and restoring any affected system files.

Additionally, ZeroLock enhances Linux security with "lockdown rules," fine-grained controls for files, processes, and network access. These rules minimize the attack surface, harden Linux endpoints, and enable MFA for SSH, even in disconnected settings, establishing a zero-trust environment.

In the unfortunate event of an attack, ZeroLock provides file rollback, swiftly restoring all lost files and ensuring minimal downtime for critical systems. This can happen automatically or at a push of a button, and all without having to store our client's data.

Lastly, it's not just about what we can do but how we can do it. We focus on operationalization by ensuring ease of deployment and management, all while running on extremely low overhead and only 50MB of memory.

ZeroLock enhances Linux security with "lockdown rules," fine-grained controls for files, processes, and network access.

TAG: In the security space, the term "single pane of glass" is prevalent. Overburdened Cybersecurity teams want to simplify and streamline. What do you think about that approach?

VALI CYBER: I empathize with the perspective. However, there are greater risks in deploying a weaker solution on Linux systems. With the continued push to the cloud, we're seeing increased attacks on Linux. To protect its most critical data, a company must consider a best-of-breed approach combining the best solutions for each OS used—which is why integrations are so important.

Through its API, ZeroLock offers seamless integration with third-party systems, allowing easy connectivity with Security Information and Event Management (SIEM) systems, Security Orchestration, Automation, and Response (SOAR) platforms, data lakes, data warehouses, and centralized threat-hunting platforms. In fact, we're proud to announce a recent integration project with SwimLane. To see that in action, join us for a free webinar on November 9.

TAG: How portable is ZeroLock? What architectural frameworks are best suited?

VALI CYBER: Running on Linux distributions with kernel 3.5 or higher, ZeroLock is versatile and integrates seamlessly with various architectures, including public, private, and hybrid clouds, dedicated servers, virtual machines, containerized workloads like Kubernetes, and air-gapped environments. Its lightweight nature ensures easy deployment across diverse platforms, offering robust security regardless of the underlying system.

Managing ZeroLock is a streamlined process. Notably, the ZeroLock Agent requires no reboot for installation or updates, and a single instance can effortlessly scale to accommodate over 20,000 agents on a modestly sized server, as verified on an AWS t2-xlarge instance.

TAG: In the context of GDPR and CCPA, how does Vali Cyber ensure compliance while safeguarding sensitive data?

VALI CYBER: We strongly emphasize data privacy and regulatory compliance, specifically aligning with the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA). Vali Cyber enforces rigorous access controls and user permissions through its ZeroLock™ platform, ensuring that only authorized personnel can access sensitive data. Role-based access control (RBAC) mechanisms enable organizations to customize access based on job roles and responsibilities. Plus, multi-factor authentication provides an extra layer of user verification.

Secondly, the ZeroLock Management Console platform incorporates comprehensive audit trail capabilities, meticulously logging all sensitive data access activities and processing.

This transparency empowers organizations to demonstrate compliance by providing a clear audit trail of data handling. Vali Cyber collaborates with organizations to establish and implement data retention policies that adhere to regulatory requirements. Organizations can manage their data according to GDPR and CCPA guidelines by automatically deleting or archiving data per predefined rules.

Lastly, the ZeroLock Management Console is deployed on customer infrastructure within the specified geographic region to address data residency requirements. This strategic approach ensures compliance with the relevant data residency regulations, offering organizations additional assurance.

TAG: Are there any other features you'd like to highlight?

VALI CYBER: Sure. I'll focus on two. The first is that the ZeroLock Management Console provides multi-factor authentication and integration with centralized single-sign-on (SSO) authentication solutions. ZeroLock also uniquely enforces multi-factor authentication (MFA) over SSH as an additional layer of security to ensure secure access to Linux systems protected by ZeroLock.

Why is this important? 50% of all attacks on Linux use compromised credentials. Multiple authentication factors reduce unauthorized access risk and strengthen overall security, allowing administrators to define and enforce specific authentication policies. MFA capabilities are available both for SaaS and customer infrastructure deployments.

The second feature is extremely low overhead. Everyone strategizes about lowering cloud costs, but they should consider the unrecognized cloud cost of their security products. We developed ZeroLock with low overhead in mind, then built SecurityPerf, an open-source benchmarking tool to help us accurately measure overhead.

In our testing, ZeroLock runs at <5% overhead. What's shocking is hearing from security teams that their solutions can have overheads exceeding 50%, which essentially means every cloud server purchased only delivers half its potential productivity—significantly affecting the company's efficiency and bottom line.

AN INTERVIEW WITH KEVIN KENNEDY
SVP PRODUCT, VECTRA AI

AI-ENHANCED HYBRID CLOUD THREAT DETECTION AND RESPONSE STRATEGIES

In an interview conducted by the TAG analyst team, we discussed Vectra AI's proficiency in using AI across threat detection, investigation, and response. As the digital landscape becomes increasingly complex, Vectra AI's pragmatic approach to leveraging artificial intelligence for identifying and responding to hybrid and multi-cloud cyberattacks have gained prominence.

The conversation below covers the fundamental methodologies that underpin Vectra AI's mission to deliver the most accurate attack signal so SOC teams can respond at speed and scale. Vectra AI offers insights into practical strategies for staying ahead of evolving threats and safeguarding critical hybrid and multi-cloud environments

TAG: What differentiates Vectra AI's threat detection and response platform in identifying and mitigating threats across diverse hybrid environments?

VECTRA AI: Our differentiation is in our mission – to deliver the most accurate attack signal to enable defenders to investigate and respond at speed and scale. We believe integrated AI-driven attack signals at speed and scale are the only effective defense against modern hybrid attacks, which take advantage of the growing attack surface to gain access and progress using evasive methods designed to thwart rules and signatures. Our approach is rooted in the three Cs: Coverage, Clarity, and Control.

Coverage across the entire attack surface is paramount to early detection, but getting high-quality coverage everywhere is hard. AI is critical to accurately finding attack signals for modern techniques. We have invested over a decade to deliver native detection for networks, identity, public cloud, and SaaS.

Seeing in-progress attacks in real time on each of these attack surfaces is game-changing for our customers. In addition to Vectra, most use EDR, email security, web security, CASB, and other tools, which also throw off detections of varying quality and with siloed context. They struggle to make sense of all of this, which leads to the next challenge: Clarity.

Clarity requires munging all individual detections together to deliver an accurate attack signal that connects the dots for responders and separates signal from noise. We've done this for the Vectra

We believe integrated AI-driven attack signals at speed and scale are the only effective defense against modern hybrid attacks, which take advantage of the growing attack surface to gain access and progress using evasive methods designed to thwart rules and signatures.

native signal using another AI engine that automatically determines security relevance, profiles the combination of techniques used, and factors in the importance of the entity to point the SOC to the most urgent incidents. In the past, we've told customers to correlate this with other detection signals in their SIEM, but this has been futile for most. We're now applying the same AI prioritization methodology to 3rd party signals: EDR, email security, SASE, etc.

What good is coverage and clarity if you cannot control the attack in progress? Control comes from integrated, automated, co-managed investigation and response actions that arm SOC teams to move at the speed and scale of hybrid attackers. We put 360 degrees of attack context at analysts' fingertips so they can investigate attacks in real time. Once analysts have the confidence to take action, they can flexibly execute automated or manual isolation or containment of the attacks.

Without coverage, you won't get clarity. Without clarity, you will never have control. Vectra AI is about providing all three.

TAG: Can you provide examples of organizations that have achieved significant improvements using Vectra AI's solutions?

VECTRA AI: We partner with over a thousand enterprises worldwide to improve detection and response times, including Blackstone–the world's largest alternative asset manager. Our Attack Signal Intelligence enabled Blackstone to reduce the alert volume by 90% and achieve coverage for over 50 new M365 and Azure AD attack techniques in a single day. Without our solution, their expert team faced a timeline of over six months to develop this coverage, leading to an ongoing maintenance drain. Another example is Lamb Weston-a leading global food supplier–which relies on Vectra's Attack Signal Intelligence and MDR services. With Vectra MDR, Lamb Weston closed threat detection gaps in their Azure environment and reduced SOC workload, which freed their teams to focus more on proactive defense and less on putting out fires.

TAG: How does Vectra AI adapt to cyber adversaries' constantly evolving tactics and techniques to ensure ongoing threat visibility and protection?

VECTRA AI: If threat intelligence gives security the confidence to mitigate the known, Attack Signal intelligence gives security the confidence to mitigate the unknown.

Attackers' techniques for lateral movement evolve slowly after initial compromise. Fast and frequent compromise attempts require strong hybrid coverage, ensuring the system can quickly detect its presence even if attackers use new techniques or exploits.

While attack techniques post-compromise evolve slowly, they do evolve – especially in the cloud. Our expert security researchers

ensure we're on top of these evolutions. Their job is to understand unique changes in attacker behavior unique to each of these environments. The second is our MDR team. Vectra MDR analysts observe attackers' evolving techniques and emerging threats across hybrid attack surfaces. The MDR team feeds this insight to our security researchers, data scientists, and product teams so that we can adapt and evolve our detection models. We have also created a "network effect" to keep pace with hybrid attackers.

TAG: Can you elaborate on the integrations and partnerships that enhance Vectra AI's ability to provide comprehensive threat detection and response?

VECTRA AI: No one vendor can be everything to everyone when it comes to modern attacks. For example, we are not experts in the endpoint domain, so we partner with CrowdStrike, Microsoft, and other leading EDR partners to leverage their signal for detections, context for investigation context, and controls for response, and vice versa. We understand that enterprises may have built their SOC workflows in an SIEM or have invested in SOAR, so we integrate Attack Signal Intelligence with Splunk, Microsoft Sentinel, IBM Qradar, and Cortex XSOAR. Every security vendor wants to be their customers' single pane of glass when the real goal should be to help customers deliver on their outcomes no matter their pane of glass.

TAG: What role does behavioral analytics play in Vectra AI's platform?

VECTRA AI: If one challenge affects nearly every one of our customers, it's the spiral of more, i.e., more attack surfaces, blind spots, tools, alerts, false positives, evasive attackers, workload, stress, anxiety, burnout, and so on. The problem is threefold: getting high-quality detection coverage everywhere is hard, knowing what threats are a priority is a guessing game, and connecting the dots to take confident action takes too long.

Vectra AI's application of behavior-based AI/ML integrated across hybrid attack surfaces – our Attack Signal Intelligence – alleviates SOC teams' manual burdens of writing and tuning detection rules, triaging alerts, and correlating individual threat events. With Attack Signal Intelligence, SOC teams get a prioritized view of entities under attack. Behavioral-based AI/ML saves time and arms humans to do what they are best at–critical thinking, reasoning, and creative problem solving, focusing their time and talent on investigating and stopping real attacks.

ANALYST REPORTS

ANALYST REPORT

A PRIMER ON SAAS SECURITY SOLUTIONS

DAVID NEUMAN, SENIOR ANALYST, TAG

As the SaaS security market begins to take shape, TAG developed this primer to help stakeholders make informed decisions on securing their SaaS environments. This guide was commissioned by Nudge Security.

INTRODUCTION

As the digital revolution continues to reshape the business landscape, organizations of all sizes and sectors have embraced cloud-delivered infrastructure (IaaS), platforms (PaaS), and software applications (SaaS) to drive efficiency, agility, and innovation. But this rapid and often decentralized adoption of SaaS applications (by both business units and individual employees) has meant new challenges in managing security risks, maintaining compliance, optimizing costs, and ensuring that these tools genuinely deliver on their promise of transforming business operations.

This guide underscores the growing importance of SaaS security and governance platforms. These tools provide the visibility, control, and automation needed to manage and secure an organization's SaaS environment effectively, but their value extends beyond mere risk mitigation. By providing a single source of truth for all SaaS applications, a SaaS security platform can also identify redundant applications, underused licenses, and opportunities for better integration and leveraging of these tools to optimize cost and operational efficiency.

The critical differentiating capabilities of SaaS security platforms—including comprehensive visibility, automated compliance monitoring, threat detection and response, risk management, access control and identity management, integration capabilities, and actionable insights and reporting—make them essential tools for navigating the complex and rapidly evolving SaaS landscape. The adoption and effective use of SaaS security is not solely the domain of IT departments as it involves diverse stakeholders: CIOs, CFOs, CISOs, IT managers, compliance officers, risk managers, procurement managers, business unit leaders, data privacy officers, R&D, and DevOps teams. It even includes individual employees who become citizen admins for the tech they introduce to the SaaS environment. Each of these roles brings a unique perspective and set of concerns, and each stands to benefit in different ways from the insights and controls provided by a SaaS security platform.

The opportunity here, and the central premise of this guide, is that by using the SaaS security platform as both a system of record and a tool for partnership and collaboration, these stakeholders can address the challenges of SaaS adoption and unlock its full potential for driving business success. By ensuring that SaaS applications are used securely, efficiently, and in a manner that supports rather than impedes business objectives, organizations can truly leverage the transformative power of SaaS.

So whether you're a CIO looking to manage your organization's SaaS landscape, a compliance officer tasked with maintaining regulatory compliance and frequent access reviews, a business unit leader seeking to drive efficiency and innovation, or any of the other roles involved in managing and using SaaS applications, this guide is designed to help you understand the value of SaaS security platforms and navigate the process of selecting and implementing the right solution for your organization.

ADVANTAGES OF SAAS ADOPTION

Embracing SaaS carries many benefits that resonate with an organization's technical- and business-minded leaders. These advantages often drive SaaS adoption and are worth considering when selecting a SaaS security platform. Let's explore them in more detail.

Agility and Scalability to Meet Business Demands. SaaS platforms are designed for agility, making businesses nimble in fluctuating market conditions and customer needs. They allow for the swift deployment of new technology, eliminating the need for lengthy installations or substantial upfront investments in infrastructure, enabling businesses to scale their SaaS usage based on real-time demands, a crucial factor for growth opportunities and navigating market changes.

Cost Efficiency and Resource Optimization. SaaS platforms present a cost-efficient solution, operating on a subscription model that typically incurs lower initial costs than traditional software. In addition, the subscription often encompasses updates, maintenance, and customer support, facilitating predictable budgeting. Further, SaaS adoption lightens the load on IT teams, freeing them from tasks such as software installation, updates, and troubleshooting and allowing them to concentrate on strategic initiatives. This leads to enhanced operational efficiency.

Innovation for a Competitive Edge. SaaS can fuel innovation and provide a competitive advantage. SaaS providers regularly roll out new features and capabilities, giving businesses access to the forefront of technological advancements. This fosters the ability to quickly leverage new tools and features, a significant advantage in delivering exceptional customer experiences, streamlining operations, and keeping pace with market trends.

Flexibility and Accessibility for a Modern Workforce. Flexibility and accessibility are hallmark advantages of SaaS applications. As cloud-based solutions, they can be accessed anywhere with an internet connection, a vital feature in supporting today's increasingly remote and mobile workforce. Because SaaS is designed to be frictionless for any individual to use and learn, most often without requiring any specialization or certification, it also promotes collaboration among geographically dispersed teams and can often "go viral" by encouraging users to invite collaborators to use the technology.

Disaster Recovery and Business Continuity. This flexibility extends to business continuity and disaster recovery, allowing operations to persist regardless of the accessibility of physical office locations. Many SaaS applications are also designed to integrate with other business systems in no-code and low-code manners, simplifying the creation of a unified, flexible technology ecosystem that caters to diverse business needs. They also shift the shared responsibility model as functions such as system updates and vulnerability patching are now the responsibility of the SaaS provider.

RISKS ASSOCIATED WITH SAAS ADOPTION

Business units often turn to SaaS applications out of a need for agility, efficiency, and customizability, which traditional IT departments may need specific domain expertise to address. In this sense, adopting SaaS applications can be a proactive and innovative approach to solving business problems. There is also no inherent risk associated with SaaS that doesn't also apply to owned IT.

However, this doesn't diminish the fact that uncontrolled or uncoordinated use of SaaS applications can introduce security risks and compliance issues. This is where the concept of SaaS security becomes critical. An effective SaaS security and governance strategy allows organizations to embrace the benefits of SaaS while mitigating the associated risks and providing the necessary visibility and control over SaaS use across the organization.

With SaaS applications, data is typically stored on the provider's servers, which may be located anywhere in the world. This can raise *data privacy and protection* issues, particularly if the provider still needs robust security measures. Additionally, unauthorized individuals could access data if user access controls are not correctly implemented and managed.

Maintaining *compliance can be challenging*, particularly for organizations subject to regulations like GDPR, CCPA, or HIPAA. SaaS providers may store and process data in locations or ways that are not compliant with these regulations, potentially exposing the organization to penalties. Therefore, organizations must understand their compliance obligations and ensure their SaaS providers can meet them.

Application sprawl is the use of duplicative software and systems, including SaaS applications, without the knowledge or approval of the IT department. This can lead to a proliferation of unmanaged, potentially insecure applications, and can drive excessive costs, create significant security risks, and make it difficult to maintain an accurate inventory of the organization's software assets.

Access control and identity management with SaaS applications are critical. Managing who has access to what data and ensuring access is revoked when no longer needed can be complex and nuanced. Without proper access control and identity management, there's a risk of unauthorized access or inappropriate sharing of sensitive information.

Relying on *third-party vendors* for critical applications can be risky if the vendor experiences downtime, goes out of business, or fails to deliver the expected service. Moreover, if the vendor is breached, it could expose the customers' data to risk.

SaaS providers face *data loss and recovery* issues just like any organization. While SaaS providers typically have measures to prevent data loss, there's always a risk that data could be lost or corrupted due to a technical issue, cyberattack, or human error. And while some providers offer data recovery services, these may only sometimes be sufficient to recover all lost data.

Many SaaS providers offer APIs and support OAuth to allow for integration with other systems. These integration points could provide attackers with a potential entry point if they are not adequately secured. Therefore, OAuth and *API security* will continue to be a risk that must be addressed.

OAuth and API tokens are integral components of SaaS application integration, ensuring secure data exchanges without revealing user credentials. However, they could be exploited, giving unauthorized access to sensitive data. Therefore, it's essential to prioritize robust OAuth and API token management to safeguard your data against potential cybersecurity threats.

BUSINESS STAKEHOLDERS IN SAAS SECURITY

Let's delve deeper into the various business personas who would find value in a SaaS security and governance platform. Each persona plays a critical role in adopting and managing SaaS applications and their associated security posture within an organization. They each have unique responsibilities and perspectives that influence their understanding of the value that a SaaS security platform can bring. Their relevance lies in the extraordinary impact they can each have on the successful selection and implementation of a SaaS security platform.

Chief information officer (CIO): The CIO oversees an organization's IT strategy and implementation. As SaaS adoption increases, the CIO must ensure that these applications align with the organization's IT strategy and are properly managed and secured. In addition, a SaaS security platform can provide the tools needed to manage the SaaS landscape effectively, so a guide that helps them choose the right solution would be valuable.

Chief information security officer (CISO): The CISO primarily manages cybersecurity risks. As such, they would be interested in SaaS security platforms that can provide comprehensive visibility into the organization's SaaS attack surface, supply chain risk, security policies, compliance, and threats such as signs of an account takeover. A buyer's guide can help them understand the required security features and capabilities in a SaaS security platform.

IT manager: IT managers oversee day-to-day IT operations, including managing SaaS applications. They would be interested in SaaS security platforms that simplify SaaS management tasks, such as access control, identity management, user lifecycle management, and incident response. A buyer's guide could help them identify platforms that offer these capabilities.

Compliance officer: Compliance officers must ensure that the organization uses SaaS applications to comply with relevant regulations and standards. They would be interested in SaaS security platforms that monitor compliance, generate compliance reports, and automate compliance tasks, such as conducting regular SaaS access reviews. A buyer's guide would help them understand how different platforms can support specific aspects of their compliance programs.

Procurement manager: Procurement managers are responsible for purchasing decisions. They would be interested in the cost-effectiveness of different SaaS security platforms and their scalability, reliability, and vendor support. A buyer's guide could give them the information they need to evaluate and compare options.

Business unit leaders: Business unit leaders use SaaS applications to drive business operations and results. They would be interested in SaaS security platforms that can ensure the availability and performance of these applications without impeding productivity. It can help them understand the adoption and use of the SaaS they administer, so they can plan and budget accordingly.

Data privacy officers: Data privacy officers ensure an organization complies with relevant data protection laws and regulations. They oversee data privacy policies, conduct privacy impact assessments, and serve as the point of contact for individuals whose data the organization processes. With the rise in SaaS applications, data privacy responsibility extends to the cloud. Data privacy officers must ensure that sensitive data stored or processed in SaaS applications is adequately protected and that the organization's SaaS use complies with privacy laws such as GDPR, CCPA, or HIPAA.

Key considerations: The platform should provide a broad view of all the SaaS applications being used across the organization, along with categorization to identify redundant applications. It should also include information on the use of each application, which can further assist in determining which applications are essential and which are superfluous. Moreover, the platform should provide actionable recommendations for consolidating applications and reducing unnecessary expenses. It would be beneficial if the platform can also estimate potential cost savings of removing certain applications.

A UNIFIED APPROACH

In light of the emerging nature of SaaS security solutions, the focus should be on selecting tools that align with your organization's primary objectives and desired state for SaaS security and governance. This process begins with understanding the risks associated with SaaS adoption and establishing a vision of how you want to manage those risks. From there, an inventory of existing technologies, such as IAM/IdP solutions, can be leveraged to integrate with the selected SaaS security solution, ensuring seamless functionality and maximum utility.

In this strategic approach, practitioners and business leaders come together to balance the equation of risk management and operational efficiency. The ultimate aim is to empower business units with the right SaaS tools that foster innovation while maintaining security and compliance, essential in today's intricate digital ecosystem. A culture of shared responsibility becomes integral, where every stakeholder understands their role in maintaining security protocols.

By prioritizing their primary objectives and harmoniously integrating new SaaS security solutions with existing technology, organizations can enhance their security posture, maintain compliance, and optimize costs associated with SaaS applications. This strategic approach not only addresses immediate security needs but also contributes to the organization's long-term financial health and sustainability.

CONCLUSION

The rapid adoption of SaaS applications across various sectors and industries has brought new challenges in managing security risks, maintaining compliance, optimizing costs, and ensuring that these tools deliver on their promise of transforming business operations. SaaS security platforms offer a solution to these challenges. By providing a centralized view of an organization's SaaS applications, SaaS security platforms offer the visibility, control, and automation necessary to manage and secure the SaaS environment.

Beyond mitigating security risks and ensuring compliance, SaaS security platforms offer cost optimization and operational efficiency opportunities by identifying redundant applications, underused licenses, and opportunities for better integration and leveraging of SaaS tools. Thus, the critical differentiating capabilities of SaaS security platforms make them essential tools for navigating the complex and rapidly evolving SaaS landscape.

Finally, adopting and effectively using a SaaS security platform requires diverse stakeholders, including CIOs, CISOs, IT managers, compliance officers, risk managers, procurement managers, business unit leaders, data privacy officers, and DevOps teams. Each of these roles holds a unique perspective and set of concerns, and each stands to benefit from the insights and controls provided by a SaaS security platform. Therefore, organizations must work collaboratively to ensure the SaaS security platform is optimized for all stakeholders' needs, contributing to better security, compliance, cost optimization, and operational efficiency.

DevOps team: DevOps teams are responsible for developing, deploying, and managing software applications, including SaaS applications. They aim to deliver high-quality software quickly and reliably while ensuring security is embedded in the development and deployment process, a practice often called DevSecOps. DevOps teams must ensure that customizations and integrations with other systems are done securely in the context of cloud infrastructure and SaaS applications.

Individual employees: All employees benefit from understanding (1) what sanctioned tools are already being used across the organization and which citizen administrator can provide access; (2) the extent and details of their own SaaS footprint; and (3) what their own SaaS security posture looks like relative to the organization's IT and security policies, as well as guidance on how to support those policies and use SaaS applications responsibly.

DIFFERENTIATING CAPABILITIES AND ADVANTAGES OF A SAAS SECURITY PLATFORM

As digital transformation becomes the norm across industries, the security of software systems has taken center stage. A SaaS security and governance platform offers unique capabilities and advantages in addressing these concerns. Its fundamental differentiation comes from its cloud-native structure, offering comprehensive, scalable, and agile security solutions. These platforms present a paradigm shift in cybersecurity, blending security and governance. This section discusses the distinct capabilities and advantages of a SaaS security platform, highlighting how it can help organizations maintain security, agility, and resilience in the face of ever-evolving security threats.

Comprehensive Discovery and Visibility. A SaaS security platform provides a continuous overview of your entire SaaS application landscape as it changes. This unified view lets you see which applications are used, who uses them, and how they are configured, enabling effective management and control over your SaaS environment.

> **Key considerations**: Highly distributed organizations, especially those with flexible and remote work options, should evaluate vendors' discovery capabilities based on their ability to look beyond the network perimeter and corporate-managed devices to discover SaaS use. Not all SaaS discovery solutions provide the same breadth of discovery, and buyers should consider how deployment is performed. For example, agents or browser plug-ins require an additional level of effort for IT teams. Additionally, the ability to inventory applications already in use before deployment is essential. Finally, the continuous discovery of new applications versus having to provide a list of applications in use is an important differentiator.

Automated Compliance Monitoring. This is an important function that not only safeguards your data but also ensures that your system adheres to the latest compliance regulations. It simplifies the complex and time-consuming process of compliance reporting. SaaS security platforms can automate compliance checks across all SaaS applications, which is crucial in adhering to regulatory standards, such as GDPR, HIPAA, or SOC 2, helping your organization avoid potential fines and reputational damage.

> **Key considerations**: The ability to automate user access reviews such as those required for SOC 2 certification is an important function of SaaS security platforms. In addition, platforms should support the identification and grouping of applications that are in scope for different compliance regulations, ensuring that the right governance policies are applied to those apps. Real-time tracking capabilities that provide continuous monitoring and immediate alerts on any compliance deviation can mitigate risks before they develop into serious threats.

Key considerations: Look for a platform that provides customizable reporting options, allowing you to adapt reports to meet your unique needs and export them in the format you need for compliance and other reporting requirements. This can include tailoring the metrics and data presented, the report format, and the frequency of report generation. The ability to customize reports can help you focus on the information that matters most to your organization, aiding in efficient decision-making. Furthermore, the platform should offer the capacity to generate compliance reports based on specific standards like CIS or ISO to simplify the auditing process. A beneficial feature of SaaS security platforms is their ability to provide intelligent insights which should not only identify current vulnerabilities and compliance gaps but also predict future risks based on trends and patterns. This proactive approach allows for early mitigation of potential threats and enhances strategic planning.

Collaboration. Use insights from the SaaS security platform to engage with business units, understand their needs and challenges, and discuss potential risks associated with their SaaS applications. This collaborative approach encourages business units to be part of the solution rather than viewing IT as a barrier.

Key considerations: A critical consideration for promoting collaboration is the ease of use of the platform. A user-friendly interface encourages business units to interact with the platform, enabling them to understand their security postures. This, in turn, facilitates informed discussions about potential risks and mitigation. Platforms that offer clear dashboards and intuitive tools promote higher engagement and foster a collaborative environment. The platform should allow for controlled access across different departments or business units to enable various stakeholders to view and understand the security status relevant to their operations. Such transparency can drive proactive discussions and shared responsibility for security, positioning IT as a partner rather than a barrier. The platform should offer fine-grained access control to ensure users can only view and modify data relevant to their roles.

Empowerment. By providing business units with the tools and information they need to manage their SaaS applications securely, they can take greater responsibility for their SaaS security posture with oversight. This might include training on secure usage practices, providing access to the SaaS security platform for self-service security checks, triggering prompts to request that end users take specific actions, and establishing clear SaaS adoption and use guidelines.

Key considerations: An effective SaaS security platform should offer the ability to point users to educational resources and training modules to help them understand security best practices and how to use the platform effectively. This could include short tutorials or just-in-time guidance. Empowering users with the necessary knowledge and skills at the optimal time encourages greater ownership of security responsibilities and promotes a culture of security awareness throughout the organization. The platform should offer user-friendly, self-service capabilities so users can conduct security checks and manage their security settings. For instance, users should be able to view the security status of their applications or adjust security settings. This kind of user empowerment allows for quicker responses to security issues and a more decentralized, yet secure, control over the SaaS applications.

Eliminating Redundancies. A SaaS security platform's visibility into all SaaS applications across the organization can identify redundant applications. By consolidating these applications, the organization can reduce unnecessary costs.

Threat Detection and Response. SaaS security platforms should use advanced analytics and machine learning to detect unusual or suspicious behavior that could indicate a security threat. Once a potential threat is identified, the platform can take predefined actions to respond or alert your security team for manual intervention. Some platforms can even alert you to breaches of the SaaS providers you use and those in the digital supply chain of your providers. This is becoming more important as threat actors like Lapsus$ have demonstrated the ability to move across the SaaS supply chain toward high-value targets.

> **Key considerations**: Consider the platform's ease of integration with existing security systems and technology, such as security information and event management (SIEM) and security orchestration, automation, and response (SOAR). Additionally, an effective SaaS security platform should provide real-time threat detection capabilities. This means the system continuously monitors for any suspicious activities or anomalies and generates immediate alerts when potential threats are identified.

Risk Management. SaaS security platforms use advanced technologies like artificial intelligence and machine learning to identify and evaluate potential risks before they become issues. Some can collect information about a SaaS provider's security program, compliance attestations, breach history, and other relevant factors to assess potential risks and speed up vendor security reviews. This proactive approach allows businesses to effectively evaluate risks and implement preventive measures, thereby reducing the likelihood and potential impact of security incidents.

> **Key considerations**: SaaS security platforms can identify risks in applications or between applications. This is particularly true when examining OAuth grants. They can also identify risks in applications and cloud services that exist outside central governance, which might not have appropriate security controls applied.

Access Control and Identity Management. SaaS security platforms often include features for managing user identities and access controls across your SaaS applications. This can consist of identifying which apps and accounts are (or are not) enrolled in single sign-on (SSO) or multifactor authentication (MFA), identifying app-to-app integrations via OAuth, and leveraging user behavior analytics, all of which contribute to securing user access.

> **Key considerations**: The SaaS security platform should seamlessly integrate with your existing identity and access infrastructure and other SaaS applications. It should support standard protocols to ensure compatibility and minimize operational disruptions during implementation. A platform that offers prebuilt integrations or APIs can further streamline the integration process. As your organization grows or evolves, the platform should be scalable to accommodate an increased number of users, applications, and data. It should also offer flexibility to handle diverse user roles and complex access policies. The ability to scale and adapt in response to your business needs is critical to maintaining robust and effective access control and identity management over time.

Actionable Insights and Reporting. SaaS security platforms provide detailed, audit-ready reports for compliance requirements for attestation such as SOC 2, as well as actionable insights on your SaaS security posture. These insights can include highlighting updates to framework controls such as CIS or ISO, assessing MFA and SSO coverage across applications, and documenting user access reviews. These insights can help guide decision-making and security strategy and demonstrate compliance to stakeholders or auditors.

ANALYST REPORT

USING REDSEAL FOR CYBERSECURITY AND COMPLIANCE: AN INDEPENDENT ASSESSMENT

DR. EDWARD AMOROSO, FOUNDER & CEO, TAG

A recent study by independent industry analysts at TAG Infosphere concluded that the exposure analytics capabilities of the RedSeal platform—specifically, network modeling, attack path analysis, risk prioritization, and compliance management—are well-suited to reduce risk and strengthen the security posture of complex hybrid networks.

INTRODUCTION

TAG Infosphere[1] was recently engaged to independently assess the degree to which the RedSeal[2] platform supports modern cybersecurity and compliance objectives. The two-month assessment, which was held in 2023, focused on RedSeal's cyber risk modeling toward enhanced digital resilience. TAG Infosphere analysts reviewed the platform, examined RedSeal compliance support, interviewed practitioners, and performed a criteria assessment.

The TAG Infosphere team maintains and manages a portfolio of different taxonomies and models to support enterprise security assessments as well as assessments of commercial platforms for cybersecurity and compliance. The TAG Taxonomy, for example, is used by enterprise teams to review their deployment for potential gaps in coverage or areas in which architectures might be improved.

In addition, the TAG Infosphere team maintains a TAG Cybersecurity Framework (TAG CSF) which serves as a set of evaluation criteria (described below) that assists in reviewing a given commercial platform for deployment in modern enterprise network environments. Experience at TAG Infosphere suggests that the requirements included in this TAG CSF structure streamline analysis and simplify determination of a given platform's effectiveness.

[1] *Founded in 2016 by Dr. Edward Amoroso, TAG Infosphere, Inc. is a New York-based research and analyst firm that focuses on closing the trust gap between enterprise practitioners and commercial cybersecurity vendors.*

[2] *Sunnyvale-based RedSeal uses cyber risk modeling to help organizations quantify and improve cybersecurity and compliance using input from network elements such as switches, routers, firewalls, and load balancers.*

For this assessment, the results of previous security compliance framework mappings by the RedSeal team also provided insights to the overall assessment.[3] Such mappings helped to highlight the dual objectives – both security and compliance – addressed by RedSeal for the typical modern organization. It is worth noting that the assessment was designed to be applicable to both commercial enterprise as well as government agency infrastructure.

Interviews held by TAG Infosphere with various industry practitioners provided valuable context into how cyber risk modeling platforms can be best applied to meet the cybersecurity and compliance needs of the major industries.[4] These discussions also offered validation of the compliance assessments, and also helped complement the assessment conclusions drawn from the TAG CSF review of the RedSeal platform.

The primary management conclusions drawn from this independent assessment by TAG Infosphere involved the following three main findings related to use of the RedSeal network exposure analytics platform:

- **Network Complexity** – RedSeal addresses network complexity by increasing awareness and understanding of the growing number of different devices and systems that complicate modern organizations networks. This is an essential capability as organizations drive to zero trust networks in 2024 and beyond.
- **Security Controls** – RedSeal strongly supports the identification, prioritization, and implementation of the optimal, broad cybersecurity controls to be applied across a modern organization's network. As one would expect, security controls must be strong given the growing intensity of adversary offensive measures.
- **Compliance Risk** – RedSeal enables enterprise teams to address their growing liability, risk, and compliance needs through the use of cyber mappings, summary reports, and data visualization. This liability includes attacks such as ransomware and other business-impacting breaches.

The enterprise and government participants considered here were assumed to exhibit three primary environmental characteristics: First, we assume that their device profile is dynamic and changing; second, we assume that the business unit functions are non-trivial and result in a complex network environment; and third, we assume that the network includes many business and supply chain complexities, especially for third-party support.[5]

HOW REDSEAL WORKS

The RedSeal commercial platform was designed to strengthen an organization's overall network security posture. While the platform can help organizations stop hackers, as will be explained below, in their tracks and respond to incidents faster, it's also designed to help security teams operationalize network exposure management in a proactive, ongoing way. This is especially helpful in complex hybrid network environments.

More specifically, RedSeal supports cybersecurity risk and compliance objectives by enabling enterprise teams to optimize cybersecurity and compliance of their network against events such as ransomware, data breaches, and network interruptions. RedSeal works by producing customized models of enterprise networks, which can include traditional perimeters, hybrid cloud architectures, or any other arrangement of public and private cloud infrastructure.

[3] Results of RedSeal compliance mappings for NIST 800-53 rev 4, CIS, COBIT, HIPAA, HITRUST, ISO27001, and PCI-DSS are available from RedSeal upon request. The mappings produced favorable results for modern organizations who use these frameworks as the basis for developing a control management process.

[4] TAG Infosphere conducted an initial independent cybersecurity and compliance review of RedSeal in 2020, with emphasis on healthcare organizations, resulting in a positive assessment of their capability. This report outlines the results of an updated study based on advances in the platform during the past two years as well as a more general assessment of cybersecurity and compliance for modern organizations.

[5] Standard definitions of what constitutes a typical organization network are not easily identified, but perhaps the unifying aspect of the types of modern organizations included in the review is non-trivial consequence for any risks that might emerge from cybersecurity attacks or incidents.

The primary input for a network model comes from configuration files RedSeal ingests from switches, routers, firewalls, and load balancers. RedSeal integrates with public cloud and private cloud managers to include all network environments in the model. RedSeal cyber risk modeling also imports host and vulnerability data from vulnerability scanners and other sources. This is done without agents, span ports, or taps and without being in-line with production traffic.

An important feature embedded in the RedSeal platform involves attack simulation using imported vulnerability data, which helps to drive per-asset and per-vulnerability risk scores for the organization. By engaging in this type of simulation, prioritization and remediation will be more accurate and tuned to the specifics of the local environment. This is a major differentiating capability for RedSeal.

The RedSeal platform includes direct support for many functional security and compliance objectives that are increasingly important to all major industries. These include network device configuration, accurate network infrastructure mapping, finding hidden areas of the network, visualizing the network and its devices, simulating penetration tests against the network, prioritizing vulnerabilities, verifying network policies and rules, and ensuring continuous change controls (see Figure 1).

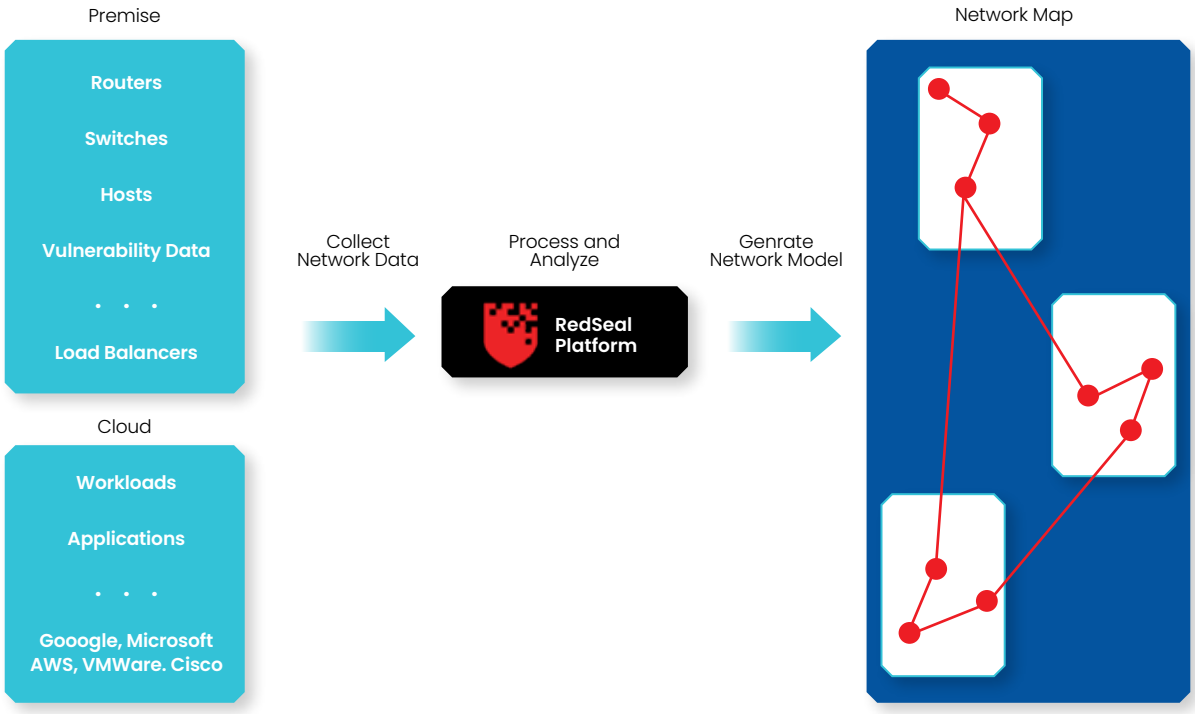


Figure 1. RedSeal Platform Overview

In addition, the RedSeal Digitial Resilience Scorecard offers a evaluation and benchmark of an organization's infrastructure and network resilience. The evaluation encompasses the completeness of network inventory, compliance status of individual network elements, and outcomes of virtual penetration tests. As the name implies, the score gauges the degree to which the network infrastructure is prepared for the next attack. It assesses factors such as accurate mapping, adherence to industry standards, and the resistance offered against attacker lateral movement subsequent to an initial breach. The score, along with the cyber risk model, validates the security posture and empowers enterprise security teams to effectively prioritize necessary network upgrades, modifications, or mitigations.

REDSEAL COMPLIANCE SUPPORT

The RedSeal platform, with its focus on network modeling and digital resilience, is uniquely suited to support the compliance needs of its customers. Specific compliance-oriented functions that help address the intense assessment scrutiny that modern organizations experience include the following:

- **Continuous Validation of Inventory** – The on-going and continuous nature of the inventory validation support from RedSeal is especially valuable for compliance programs in modern organizations. Inventory is a nagging issue in hybrid networks, for example, where new devices might be added and removed from the network. RedSeal network validation covers compliance needs in such cases.
- **Continuous Validation of Secure Configurations** – This function is central to how the RedSeal platform operates since it ingests configuration information as the basis for developing a network model. This provides a suitable compliance basis for determining the security-related aspects of such configuration information from routers, switches, hosts, and other network-resident elements.
- **Definition and Validation of Segmentation Policies** – Modern networks increasingly require segmentation, either physically through network administration or logically through micro-segmentation software controls. It is well-known that many existing modern networks are considered flat in their design, which increases risk by making key assets visible to attackers and malware on the network.
- **Quantitative Measurement of Enterprise Risk** – The calculation of a digital resilience score serves as a valuable basis for quantitative benchmarking of an enterprise team's network security posture. It is possible that the compliance program might even be organized to use this value as the basis for measuring progress. (Obviously, this would need to be established with the compliance authority.)

These platform support features for compliance should be attractive to modern network security teams – especially ones who must submit to multiple, external reviews to maintain compliance with relevant framework controls.

EXPERT INTERVIEWS

The TAG Infosphere team identified and interviewed several industry practitioners to directly gauge their level of enthusiasm for the use of cyber risk modeling toward improved digital resilience and compliance. The practitioners interviewed included experienced experts from a variety of different companies, all involving non-trivial complexities. Each was interviewed either face-to-face or using email and video conferencing.[6]

The objective in the interview process was to address three main issues: First, we wanted to understand if the security expert and their organization currently use network models as the basis for making cybersecurity decisions. Second, we wanted to determine if they viewed such method as having merit, regardless of whether it was being done now. Third, we wanted to gauge their level of interest for using this method in the future.[7]

An informal scale was used to obtain information from the experts on these issues. The results of a half-dozen interviews resulted in reasonable consensus among the experts: First, we found that 100% reported were not currently using an automated platform for building network models as the basis for their current cybersecurity decision-making. This reinforces how novel the RedSeal approach is for network security.

[6] The first round of practitioner experts interviewed during the initial phase of this security research, and updated discussions were held more recently as part of this engagement. All participants agreed to provide information in a non-attributable manner, including in most cases, with the RedSeal team. These experts are all employed by larger companies and expressed concerns that any attribution might bring legal or operational risk to the organization. TAG Infosphere thus agreed to maintain confidentiality of the interview discussions and to ensure anonymity of the expert and their team.

[7] As referenced above, TAG Infosphere maintains an advisory, coaching, consultation, and support relationship with roughly 100 major security organizations, mostly from Fortune 500 companies and government agencies. Through these relationships, it is straightforward to engage in question and answer for a given topic without too much friction or difficulty. This is how the RedSeal process in this updated phase of review was done. As one might expect, if RedSeal customers were engaged in the interview and survey process, then questions such as whether a given participant was using threat modeling for their network would obviously be in the affirmative.

Perhaps the most consequential result, however, was that 100% of those interviewed expressed agreement and enthusiasm that network modeling as exemplified by the RedSeal approach was both attractive and sensible. "This use of network modeling in the context of modern network security makes perfect sense," said one executive at a medical device company. "The approach matches up well with the needs of a modern organization."

100% OF THOSE INTERVIEWED EXPRESSED AGREEMENT AND ENTHUSIASM THAT NETWORK MODELING AS EXEMPLIFIED BY THE REDSEAL APPROACH WAS BOTH ATTRACTIVE AND SENSIBLE.

Another verbatim from a pharmaceutical executive was this: "Improving understanding of the assets in a modern network and how they are connected should be a high priority for cybersecurity teams, if only because modern networks are now so complex." This sentiment that network modeling is attractive to address the complexity of modern networks came up frequently in discussion with the experts.

REVIEWING PLATFORMS FOR CYBERSECURITY AND COMPLIANCE

Given the consequences of security breaches to hybrid networks, the security and compliance demands in all major sectors have grown considerably in recent years. This should come as no surprise since security incidents in many critical infrastructure industries could result in a major loss of assets, property, and even life. That designator – namely, whether a cyber attack could cause stress on an org and departments or actually kill a human being – has always been a prime benchmark for determining the gravity and seriousness of a security scenario.

To address this growing need, the analysts at TAG Infosphere developed the TAG Cybersecurity Framework (TAG CSF) to serve as a compact and useful basis for supporting evaluation of whether a given platform is well-suited to meet the needs of a modern organization. The TAG CSF, in contrast to many other frameworks, is focused on commercial platform evaluation, and is presented below (for use by any reader without license or request from TAG Infosphere).

The TAG CSF is best applied through its ten questions – referred to as the CSF Top Ten – to be asked by any assessment, audit, or review professional when considering use of a given commercial platform in a hybrid network setting. The TAG CSF Top Ten questions are as follows:

Question 1: Discovery – ***Does the platform assist in identifying the unique types of devices that often arise on a modern hybrid environment?*** Modern networks, especially in complicated hybrid arrangements of legacy, public cloud, secure access service edge (SASE) and software as a service (SaaS), will typically involve the introduction of a diverse assortment of different devices. Any platform designed to reduce security risk for such hybrid environments must include explicit support for identifying unique devices and offering guidance on mitigation.

Question 2: Regulatory – ***Does the platform assist in meeting the myriad of regulatory and compliance demands for modern organizations with hybrid networks?*** The intensity of regulatory and compliance requirements for most organizations, especially in critical infrastructure and government, cannot be understated. Platform support for compliance includes improved visibility, report generation, findings summaries, and risk mitigation. These capabilities streamline compliance processes for teams dealing with a growing set of requirements – including, for example, recent new cyber reporting requirements from the Security and Exchange Commission (SEC).[8]

[8] *See https://www.sec.gov/news/press-release/2023-139.*

Question 3: Design – ***Has the platform been built to strict design standards to reflect the importance of correct operation to prevent major loss of resources and assets?*** Unlike many business sectors, successful attacks on modern networks could result in significant loss of assets, resources, or even life. Such gravity of consequence must be addressed in any security platform through strict design standards to ensure safe, correct operation under any set of conditions or scenarios.

Question 4: Privacy – ***Does the platform include sufficient controls to properly protect the confidentiality of private information?*** The cybersecurity industry has come to recognize recently that sensitive data and private records have now surged ahead of credit card records in value. For example, health records are considered especially valuable to engage in insurance fraud attacks on individuals and families. This implies that security platform supporting modern networks must include specific controls to avoid compromise of patient and other private information.

Question 5: Interoperability – ***Has the platform been designed to be easily interoperable with a growing number of automated security tools deployed to enterprise?*** With the massive proliferation of technology innovations in the cybersecurity and compliance industry, it is imperative for any platform focused in this area to include the ability to interoperate. This is usually done via the inclusion of open application programming interfaces (APIs), but it can also be done by vendors through test and integration.

Question 6: Usage – ***Has the platform been designed for ease-of-use or ease-of-interpretation by any participants, such as executives, who are not cybersecurity experts?*** Most major companies and agencies employ cybersecurity experts who deal with day-to-day tactical and longer term strategic cyber issues. The platform supporting such activity must support their work, but it also must support the need to communicate results, findings, and interpretation for non-experts. This includes senior management, board members, and non-technically minded managers, employees, and other organizational stakeholders.

Question 7: Segregation – ***Does the platform support the logical or physical segregation requirements of complex hybrid networks?*** Many modern networks have developed in a so-called flat manner, with open visibility between devices scattered across the enterprise. This results in the risk of lateral traversal by adversaries after they've gained access to a target network. Most enterprise security teams are thus focused on segmenting their networks, so platforms supporting this type of design activity must easily integrate with such initiatives.

Question 8: Liability and Risk – ***Does the platform provide reduction in both liability and risk for the modern organization?*** The financial liability and potential risks associated with all major industries are well-known, which implies that cybersecurity platforms supporting each sector must include functionality that supports liability and risk reduction. Obviously, it goes without saying that such platforms must never increase liability or risk through single points of failure or other design aspects.

Question 9: Third-Party Review – ***Does the platform support on-going review, analysis, and assessment by third-party assessment teams?*** The requirements to review, analyze, and assess modern networks for vulnerabilities has intensified in recent years with the growing liability and threat. Platforms deployed across complex hybrid networks must include provisions to support the scrutiny requirements of third-party auditors, assessors, testers, and regulators.

Question 10: Evolution – ***Has the platform been designed to evolve with the inevitable innovations occurring in technology, such as artificial intelligence?*** As one might expect, exciting new innovations emerge regularly for protecting modern networks. The recent surge of interest in ChatGPT, for example, raises many questions related to cybersecurity. As a result, any commercial platform designed to interoperate with other systems on a modern network must be sufficiently flexible to adapt to future security and functional innovations.

As suggested above, the TAG CSF Top Ten provides a suitable means for assessing the suitability of the RedSeal platform for use in modern networks (see below). An advantage of the TAG CSF for this effort is its focus on commercial platforms, versus the more general frameworks that address issues outside the general scope of a platform assessment (e.g., whether a security team has proper staff recruiting processes, etc.)

The rubric recommended by TAG Infosphere for use in assessing commercial platform suitability for modern networks based on the TAG CSF is the following:

1. **Direct Coverage** – This is the greatest level of coverage for a given platform with respect to any of the questions. The platform should clearly and effectively cover the TAG CSF question being addressed.

2. **High Level of Support** – This is a high level of coverage but might rely on adjacent or complementary controls or functions to cover the TAG CSF question clearly and effectively being addressed.

3. **Complementary Support** – This involves a platform offering adjacent or complementary control to other functions that are more directly addressing the TAG CSF question being addressed.

4. **Not Applicable** – This involves the platform not being deemed applicable to a given TAG CSF question being asked. This does not imply any negative impact, but rather just a non-applicability.

The use of the TAG CSF and associated rubric above require that the assessment team use their judgment to make suitable determinations. The TAG Infosphere team recommends conservative estimates, which usually demand some tangible evidence of support before a platform is given credit for one of the four values included in the TAG CSF rubric. As stated above, readers are welcome to use the questions and interpretations listed above for their own local platform assessments.

TAG CSF REDSEAL ASSESSMENT

The RedSeal platform was analyzed in detail using TAG CSF as the basis for assessment. Each major functional component was cross-referenced with the requirements to determine suitability of the RedSeal platform to protect modern network assets. Below is a brief summary of TAG Infosphere's results and justification for the questions.

Question 1: Discovery – ***Does the platform assist in identifying the unique types of devices that often arise on a modern hybrid environment?***

Result: Direct Coverage.

Justification: The ability to identify unique device types is one of the great strengths of any network modeling solution, including the type supported by the RedSeal platform. By creating a unique connectivity map with associated meta-data and information for a given modern network, RedSeal serves to highlight unexpected network devices that might exist.

Question 2: Regulatory – ***Does the platform assist in meeting the myriad of regulatory and compliance demands for modern organizations with hybrid networks?***

Result: High Level of Support.

Justification: The RedSeal platform provides highly effective network models that can complement the needs of external regulatory and compliance reviewers. Such visibility can easily ensure a successful assessment engagement with lower cost, less review time, and fewer demands on the operational modern network teams.

Question 3: Design – ***Has the platform been built to strict design standards to reflect the importance of correct operation to prevent major loss of resources and assets?***

Result: High Level of Support.

Justification: Since RedSeal is focused on digital resilience, it is specifically focused on correct operation. Its design standards appear to be word-class[9] and its focus on network modeling will result in increased assurance that a given modern network does not include unintended components or devices.

Question 4: Privacy – ***Does the platform include sufficient controls to properly protect the confidentiality of private information?***

Result: Complementary Support.

Justification: Since the RedSeal platform does not store sensitive user credentials, customer records, or other private data, it does not include the associated burden of protection. For the data it does include, however, the system does an acceptable job of ensuring protection from unauthorized access or use.

Question 5: Interoperability – ***Has the platform been designed to be easily interoperable with a growing number of automated security tools deployed to enterprise?***

Result: Direct Coverage.

Justification: Interoperability is directly supported in RedSeal because it creates its models easily and flexibly, regardless of changes to the underlying modern network. In fact, as the network changes, the power of the RedSeal solution would appear to become more obvious to security and network teams.

Question 6: Usage – ***Has the platform been designed for ease-of-use or ease-of-interpretation by any participants, such as executives, who are not cybersecurity experts?***

Result: High Level of Support.

Justification: Usage, administration, and interpretation by non-experts is supported by RedSeal since the tool abstracts complex network data into more meaningful information that can be absorbed by non-experts. Reviewing network documentation might be tough for many participants in the executive suite or who have little technical background, but RedSeal models might make this more feasible.

Question 7: Segregation – ***Does the platform support the logical or physical segregation requirements of complex hybrid networks?***

Result: Direct Coverage.

Justification: Logical and physical segregation require a network modeling task such as supported by RedSeal. This implies not only direct coverage for this requirement, but also necessary coverage, which suggests that RedSeal modeling is uniquely necessary for any network or workload protection redesign.

Question 8: Liability and Risk – ***Does the platform provide reduction in both liability and risk for the modern organization?***

Result: High Level of Support.

Justification: Effectively supporting increasing cyber liability and risk concerns in major industries such as banking and healthcare demands the existence of accurate documentation on the network infrastructure supporting a given modern organization. RedSeal thus provides a high level of support for this liability and associated TAG CSF requirement. Documentation of network infrastructure has been a difficult and nagging issue for security experts for many years. The support from RedSeal is a welcome addition.

[9] The TAG Infosphere team did not perform a detailed code or low-level software analysis of the RedSeal platform and did not perform detailed audits of RedSeal software development lifecycle processes. Instead, high-level information on these areas was collected and reviewed by the TAG Infosphere team during the assessment period and was used as the basis for the TAG CSF judgment.

Question 9: Third-Party Review – ***Does the platform support on-going review, analysis, and assessment by third-party assessment teams?***

Result: High Level of Support.

Justification: On-going review, analysis, and assessment by third parties is enhanced by network maps and models along the lines of what RedSeal provides. This implies a high level of support for this TAG CSF requirement. It also helps to mitigate one of the most difficult security threats that any major company or government agency faces in the coming years – namely, the challenge to deal with suppliers, partners, and other third parties.

Question 10: Evolution – ***Has the platform been designed to evolve with the inevitable innovations occurring in technology, such as artificial intelligence?***

Result: High Level of Support.

Justification: Innovation in cybersecurity, networking, and application support demands that platform provide for flexible open interfaces. The RedSeal platform works with changing modern network infrastructure and is hence highly supportive of innovative new capabilities for security or other functions.

HSCF Factor	Assesment
Q1: Discovery	Direct Coverage
Q2: Regulatory	High Level of Support
Q3: Design	High Level of Support
Q4: Privacy	Complimentary Support
Q5: Interoperability	Direct Coverage
Q6: Usage	High Level of Support
Q7: Segregation	Direct Coverage
Q8: Liability and Risk	High Level of Support
Q9: Third-Party Review	High Level of Support
Q10: Evolution	High Level of Support

Figure 2. Summary of RedSeal Assessment Findings

REDSEAL FOR HYBRID ENVIRONMENTS: ASSESSMENT FINDINGS SUMMARY

This independent TAG Infosphere assessment of the degree to which the commercial RedSeal platform supports modern cybersecurity and compliance objectives in modern hybrid network environments, produced the following conclusion:

Finding 1: RedSeal provides effective cybersecurity enhancement for modern hybrid networks.

This finding suggests that prevention, detection, and response to cyber threats in a modern network environment is assisted through use of the RedSeal platform.

RedSeal cyber modeling provides a comprehensive roadmap for modern organizations to address the issues targeting the sector. Modern organizations would thus be wise to initiate such cyber modeling to reduce risk, and to help reduce the complexity that characterizes the typical network environment consisting of legacy assets, cloud-based infrastructure, SaaS-based applications, and third-party support. Specific areas where direct coverage is offered includes support for discovery, interoperability, and segregation, as determined through the TAG CSF assessment.

Finding 2: RedSeal supports enhanced compliance management for modern networks.

This finding suggests that the intense compliance needs of cybersecurity, compliance, and network teams are greatly assisted through use of the RedSeal platform.

RedSeal offers reporting, visibility, and metrics that are perfectly suited to address the requirements of modern cybersecurity and compliance activities. Major framework certifications, in particular, will benefit from the deployment and use of RedSeal, as evidenced by the extensive feature mapping. As compliance regulations and requirements increase, it is likely that the type of support offered by RedSeal will increase in relevance.

Finding 3: RedSeal supports increased digital resilience for modern networks.

This finding suggests that the digital resilience focus of the RedSeal platform reduces the risk of cyber threats, especially ones that might degrade modern network operation.

The RedSeal goal of helping enterprise teams, especially ones with complicated hybrid networks, achieving digital resilience offers an excellent means to orchestrate and synthesize cybersecurity and compliance objectives using a common platform. This reduces the seams that often exist between security and compliance.

USING REDSEAL FOR CYBERSECURITY AND COMPLIANCE: CONCLUDING REMARKS

In conclusion, as should be evident, this study by independent industry analysts at TAG Infosphere has concluded that the exposure analytics capabilities of the commercial RedSeal platform—specifically, network modeling, attack path analysis, risk prioritization, and compliance management—are well-suited to reduce risk and strengthen the security posture of complex hybrid networks.

Enterprise teams are encouraged to be in touch with the RedSeal team directly for additional information and a demonstration of the platform (*see https://page.redseal.net/demo-page*). In addition, TAG Infosphere analysts are always available to provide assistance in source selection for commercial cybersecurity platform selection, portfolio rationalization, and expert research and advisory services (see *https://www.tag-cyber.com*).

ANALYST REPORT

THE EVOLUTION OF CSPM REQUIRES REAL-TIME CONTROLS

JOHN J. MASSERINI, SENIOR RESEARCH ANALYST, TAG

The existing cloud security space is flooded with single-issue solutions (security posture management, data security, vulnerability management, etc.) that do little to provide a security team with insight into the overall risk of an enterprise's cloud environment, and what should be done about it. Multi-cloud environments (AWS, Azure, GCP) along with hybrid clouds (i.e internal VMware, Kubernetes) are posing challenges to many of the cloud security solutions on the market today.

In this report, we will review the challenges of securing a modern cloud-based infrastructure and why a comprehensive, real-time discovery and alerting solution is needed.

INTRODUCTION

Let's face it, evaluating the cloud security space is a challenging proposition. Do you need a Cloud Security Posture Management (CSPM) platform, a Cloud Workload Protection Platform (CWPP), a Cloud Native Application Protection Platform (CNAPP), or a combination of all of the above? Are you a user of a single cloud, or are you a hybrid cloud power user? Do you integrate public cloud offerings with your internal VMware, Red Hat, or Microsoft virtual infrastructure? The reality is that the more fractioned, interwoven, and cross-dependent managing an environment becomes, the harder and more complicated it is to protect.

Any security professional will tell you that complexity breeds insecurity. Developers and cloud security teams should not have to interpret risks from different platforms, from different vendors, in order to try to understand where what needs to be fixed, and why. Having one solution for cloud posture management and another for

workload protection is just setting the stage for overlooked vulnerabilities and misrepresented risks. What today's modern enterprise needs is a single platform, one that manages cloud posture, can detect threats and vulnerabilities in workloads, and intelligently baseline applications to prevent zero-day attacks and eliminate drift. What the industry does not need are more acronyms that are strictly defined by only a small piece of functionality.

COME TOGETHER.. RIGHT NOW..

As some famous person in a pretty well-known band once said, "Come together, right now.."

The ever-changing cloud security industry is finally showing signs of maturing into a cohesive, fully integrated platform by which insight and protection of the environment can be achieved. Bringing all of those pieces of individual functions together in a homogeneous platform is the only true way to manage the expanding attack surface of the cloud. From configuration drift to identity risks; vulnerability patching to anomalous behavior; having a proverbial single pane of glass to see everything within your cloud infrastructure is critical.

When evaluating the overall product functionality of cloud security solutions, it in many ways harkens back to the early days of network security where we had nothing more than an IDS to let us know when bad things happened. Security analysts would get an alert, do some quick triage, then hop on over to the firewall or proxy and manually put a block in place. Today we have active prevention systems based on machine learning and SOAR platforms to automate responses.

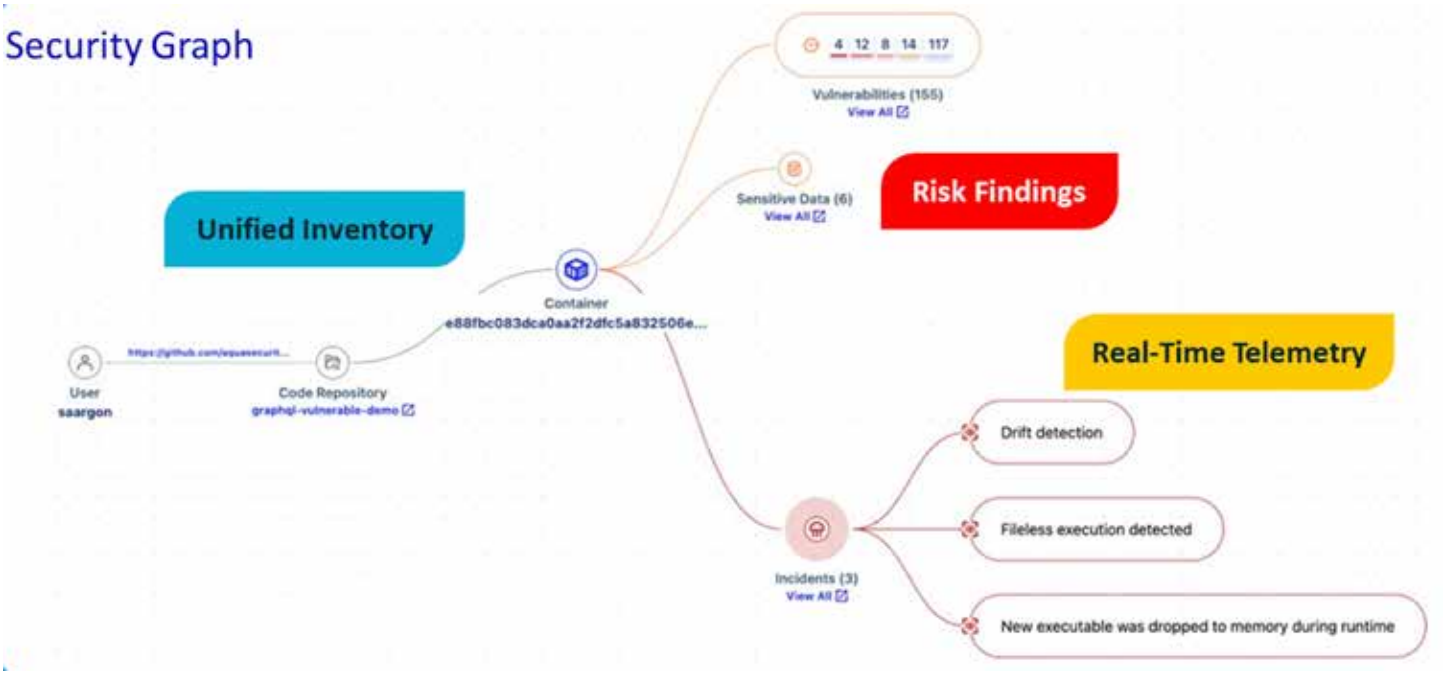
THE AQUA REAL-TIME CSPM SOLUTION

Agent vs Agentless: It's time to get real with real-time protection
When we look at the typical agentless cloud security approach, it involves a regularly scheduled scan of your cloud environment to identify risks. Depending on how aggressively the enterprise wants to manage its cloud, these scans can run daily, weekly or even monthly, but in the end, the snapshot is always just a point-in-time analysis of the environmental risk. Unfortunately, those scans incur a significant cost from the cloud provider, so balancing the expense versus the risk is an ongoing effort for most teams.

Recently, Aqua announced the addition of a real-time protection sensor to their already broad, agentless cloud security solution. The goal of the sensor is to provide real-time assessments of your workloads, the applications running on them, and visibility into any active, real-time workload modifications. Unlike the agentless solution, the sensor provides ongoing telemetry to identify unapproved configuration changes, malware activity, and fileless execution activities, providing immediate alerts via a dashboard or direct connectivity into your SIEM for monitoring via your existing Security Operations Center.

Before we get into the details of how all of this comes together, let's address the elephant in the room. There are few terms in the technology space that strike as much fear and loathing into a system administrator as the term 'agent'. And, while there may be justification for that feeling in legacy infrastructure environments, Aqua's eBPF (extended Berkely Packet Filters)[1] agent, referred to as their 'sensor', is just about as lean and unobtrusive as one can be. By leveraging eBPF, Aqua's sensor can monitor and control the entire system such as network, files, memory, and more without crashing the kernel or disrupting the performance – all for less than 1% of CPU performance

Aqua's sensor takes advantage of eBPF to instrument activities within the kernel and monitor activity. By leveraging the native eBPF interface, the agent is capable of monitoring network traffic, application execution, resource usage, and kernel interactions in real time with very light overhead. This tight integration with the kernel gives Aqua's agent the ability to alert on behaviors associated with a multitude of issues such as fileless malware execution, container drift, cryptomining, and Denial-of-Service attacks, amongst other things.



By no means does this imply that agentless scanning has gone the way of the dinosaurs. In fact, agentless scanning provides key intelligence around your entire cloud environment, such as attack surface management, identity and trust configurations, and sensitive data discovery – telemetry that can only come from scanning. But it is just the first step to securing your environment, not the end goal.

By combining the benefits of environmental and asset-based data which agentless scanning provides with the insights of runtime application-level activity from sensor-based telemetry, Aqua is able to provide a unique insight that most other cloud security providers cannot. Additionally, since sensors collect and analyze security information on the workload, scanning costs are significantly decreased over the continual-scan model.

Many points, one cohesive action

As the cloud security space matures, the functional differences between CSPM and CWPP are narrowing. There is little doubt that the evolution of cloud security toward a holistic CNAPP solution is the goal, and this is the first step to that end.

As CSPM solutions interrogate more of a workload's functionality and configuration, CWPP platforms are becoming much more aware of the cloud environment they are running, resulting in functional overlap between the sectors and confusion among the customers. For anyone who has spent time in the cybersecurity industry, a fundamental belief is that 'complexity breeds insecurity and risk' – and cloud environments are no different. If any platform has a chance of truly identifying issues within a cloud environment, it must cohesively integrate all aspects of risks into a single risk mitigation platform.

DevOps Integration

While understanding the full scope of risk within your cloud infrastructure is crucial, the ability to automate the remediation of those risks is absolutely essential in such an ephemeral environment. When we consider the agent/agentless dynamic in uncovering issues, it becomes clear how automating issue resolution by highlighting the code in question in the CI/CD pipeline and tying it to the issue being identified in runtime is no longer a 'nice to have', but rather an expectation of both DevOps and the security teams.

Since most workload configurations are stored 'as code' in standard DevOps repositories, the ability to detect changes, drift, or configurations is a necessity. Additionally, the ability to restore, or otherwise automatically correct configuration files mitigates a substantial portion of the risks faced within cloud environments today. By natively integrating with most of the leading DevOps repositories, Aqua is able to identify vulnerabilities, risks and even live attacks with the cloud and tie them all the way back to the code repository, easing the burden on the DevOps team as well.

Furthermore, this functionality, combined with the agentless scanning feature, can ensure that any new workloads automatically contain the real-time sensor, ensuring end-to-end risk mitigation with zero impact on the development lifecycle.

When you evaluate the benefits of real-time agents combined with the deep scanning technologies Aqua provides, you quickly realize the value of a fully integrated, cohesive CNAPP solution.

THE ENTERPRISE ACTION PLAN

The consolidation of CSPM and CWPP into a single enterprise platform will enable most organizations to finally gain full visibility into their cloud environment. While understanding the risks within the cloud environment is crucial, incorporating that configuration with the risks of the individual workloads allows a far deeper understanding of the entire environment, rather than just siloed parts of it. While the consolidation of cloud security platforms is obviously beneficial, the ongoing maturation of the market will result in organizations looking for more tightly integrated CNAPP solutions. Aqua's real-time CSPM solution provides an initial step into CNAPP as the functionality of CSPM/CWPP solutions continues to converge.

As such, a solid deployment strategy that takes full advantage of both agent and agentless scanning must be developed.

When implementing solutions such as Aqua, an enterprise should consider the following:

Agent/Agent-less scanning are not mutually exclusive:
As we've laid out, agentless scanning has its benefits as well as its weaknesses. Agent-based reporting also has its share of pros and cons. However, the combination of the two provides not only the breadth of coverage that agentless provides but also the onboard workload monitoring that agents provide. So, while the CSPM space has been heavily reliant on agentless scanning since its inception, the benefits of combining agent-based telemetry with agentless scanning provide far deeper insights and understanding than one, or the other, could provide. Enterprise teams can benefit significantly by leveraging both techniques to uncover previously unknown risks buried deep within the cloud environment with very little additional overhead or developer burden.

Integration into the CI/CD pipeline is essential:
One concern that is quickly raised when mentioning 'agents' is the time it takes to deploy them across the entire cloud asset base. Aqua's integration with most of the popular DevOps platforms enables integration into the CI/CD pipeline to ensure any workload that comes online has the agent pre-installed. Additionally, when agentless scanning takes place, any workload that does not have an agent is automatically flagged for an update to include the agent in the future. Aqua integrates with all of the leading Terraform, Docker, and Kubernetes platforms to ensure that new containers are fully configured and deployed in a secure manner.

Real-time alerting will need appropriate monitoring:
While the benefits of real-time workload protection have been long awaited, the potential downside is the potential for a sudden influx of unexpected alerts. When dealing with real-time agents, it is absolutely critical that the platform offers a cohesive integration with the leading SEIM solutions. While

historically, the DevOps teams managed the entire cloud environment, more and more enterprises are shifting the ownership of alerts and incidents to the Security Operations Center (SOC) for monitoring and the security incident response team for issue resolution. Since most enterprises have a single point of log collection and management that drives the SOC, having your cloud workloads integrate with the existing infrastructure is a crucial success factor. Aqua has built-in support for all of the leading SEIM solutions to ensure a quick and easy SOC integration.

Embrace Automation:
In mature DevOps organizations, having several dozen releases each week is not uncommon. Unfortunately, with such a rapid pace of deployment, security teams are often challenged with trying to figure out how to patch or otherwise secure the workload as it makes its way to production. Modern cloud security platforms must integrate into the DevOps cycle to empower the developers to remediate security issues during the testing and pre-production phases rather than in production. Aqua's solution can identify the top security issues that occur within the CI/CD process and provide real-time feedback to the developers via Slack or Jenkins. This collaborative approach not only enables the developers to understand where issues are before production but also empowers security teams to keep pace with deployment schedules. With the context of the runtime sensor, the list of issues can be better prioritized, reducing the seemingly never-ending list of application vulnerabilities to those that truly matter.

Microservices need attention:
One of the most drastic changes that DevOps practices introduced is the concept of microservices. By definition, a microservice is a small, autonomous application that serves a single function that is typically provided via API calls. The significant benefit of leveraging microservices is that, since they are tiny, stand-alone applications, they can be enhanced, upgraded, and patched without impacting any other service. Unlike the days of large, monolithic applications which requires regression testing of the entire application for each release, testing a microservice is comparatively quick and painless. Unfortunately, these same microservices can also have application-level vulnerabilities which could compromise not only the service itself but calling applications as well. As such, ensuring your cloud security platform can identify and analyze microservices is a critical functionality that should not be overlooked.

CONCLUSION

As more applications and services are moved to cloud infrastructures, security teams would be well served to have a single solution that can provide all aspects of risk mitigation, from cloud configuration, to microservices, and workload protection. The Aqua solution not only identifies risks within the cloud and the workloads, but its tight integration with the CI/CD pipeline makes it an excellent solution for mature DevOps shops who are looking to take their risk mitigation strategies to the next level.

[1] https://ebpf.io/what-is-ebpf/

ANALYST REPORT

BREAKING NEW GROUND: ADVANCING LINUX SECURITY AND RESILIENCE IN THE ENTERPRISE

DAVID NEUMAN, SENIOR ANALYST, TAG

INTRODUCTION

Digital transformation depends on scalable and resilient enterprises. Businesses increasingly rely on Linux environments to drive their core operations. Linux's flexibility, reliability, and cost-effectiveness underpin many vital processes. Yet, with cybersecurity constantly evolving and threats diversifying, the traditional methods that once stood as the cornerstone of Linux security have become notably insufficient. A compromise in Linux security can now directly impact an organization's bottom line, often manifesting as service disruptions, financial losses, and reputational damage.

No one can overstate the significance of customer trust in this equation. Whether overtly aware of it or not, customers place immense trust in organizations when sharing their data. A single security breach can jeopardize this data, eroding hard-earned trust. In today's competitive market, the assurance of data safety has transitioned from being just a matter of compliance or best practice to a strategic advantage.

There's an undeniable link between Linux security and successful business outcomes. It's not just about countering cyber threats but about safeguarding the integrity and continuity of our business operations. Modernizing our Linux security approach is not merely a recommendation; it's an imperative, directly influencing your ability to honor your customers' trust. The subsequent sections of this report will explore these themes in depth, offering insights, strategies, and actionable recommendations.

THE IMPERATIVE OF MODERN LINUX SECURITY IN THE AGE OF DIGITIZATION AND TRUST

Linux is critical to internet operations, largely due to its open-source nature. This transparency fosters a sense of trust and community collaboration and accelerates problem-solving and innovation. The fact that Linux is freely available means businesses, particularly startups, can operate at scale without being burdened by significant infrastructure costs. But it isn't just about cost-effectiveness. Linux boasts unparalleled stability, robust security, and modularity, allowing it to be tailored for many internet applications. This adaptability and its inherent scalability make it an ideal choice for the ever-expanding internet landscape. Moreover, its widespread adoption has created a self-sustaining cycle, where its dominance on the internet

further drives its evolution and use. As the digital world evolves, Linux remains poised at its forefront, a testament to its foundational principles and the vibrant global community that supports it.

The digital infrastructure of businesses has taken center stage. With its adaptability, reliability, and cost-effectiveness, Linux has emerged as the keystone of many enterprises' digital architecture. This shift isn't merely technological; it signifies a broader transformation where businesses, from startups to global conglomerates, lean heavily on digital platforms for everything from customer engagement and product delivery to data analytics and innovation. Yet, with great power comes significant vulnerability. As Linux systems underpin a broader range of critical operations, the potential fallout from security breaches has escalated dramatically. No longer are we dealing with isolated IT incidents; today's breaches can cripple supply chains, disrupt global operations, and paralyze customer interfaces. And the cybersecurity landscape is dynamic. Threat actors are more sophisticated, employing advanced techniques that can bypass traditional security measures, including the following:

- **Advanced Persistent Threats (APTs):** Historically associated with state-sponsored entities, APTs are prolonged, targeted attacks aiming to steal, spy on, or disrupt operations. These attackers are often well-resourced, employing sophisticated techniques to gain entry, stay undetected, and achieve their objectives over extended periods.
- **Ransomware Evolution:** While ransomware is not a new threat, its tactics have evolved. Initially, attackers encrypted victims' files, demanding a ransom for decryption. Today, they encrypt and exfiltrate data, threatening public exposure or sale if ransoms aren't paid. This 'double extortion' magnifies the pressure on organizations to comply.
- **Supply Chain Attacks:** These sophisticated attacks target vulnerabilities within the supply chain. Attackers can access their primary target by infiltrating a trusted vendor or supplier. The 2021 SolarWinds attack exemplifies the potential scale and impact of such threats.
- **Insider Threats:** Not all threats originate externally. Disgruntled employees, contractors, or business partners with malicious intent or those simply negligent can inadvertently become a significant security risk, causing data breaches or system disruptions.
- **IoT Vulnerabilities:** The proliferation of Internet of Things (IoT) devices has expanded the attack surface. Many of these devices, running on Linux-based systems, need to be more adequately secured, offering an entry point for attackers into broader enterprise networks.
- **Zero-Day Exploits:** These are attacks targeting undisclosed vulnerabilities in software or hardware. By their nature, zero-day vulnerabilities are unknown to the product's vendor, giving them no time (zero days) to fix the flaw before it's exploited. With its vast array of distributions and open-source nature, Linux isn't immune to such vulnerabilities.
- **Misconfiguration Exploits:** Misconfigurations can occur as organizations rapidly adopt cloud services and infrastructure. These unintentional settings can expose databases, storage buckets, or critical data unprotected, making them low-hanging fruit for opportunistic attackers.
- **Credential Stuffing and Phishing:** While not Linux-specific, these methods have evolved in sophistication. Attackers use leaked credentials to breach systems or employ convincing phishing campaigns targeting Linux administrators to gain system access.

Data security and trustworthiness become differentiators in a modern marketplace where choices abound. Consumers are increasingly discerning, factoring in data protection practices when choosing service providers. This shift positions Linux security as a back-end IT concern and a front-and-center business strategy. Ensuring robust Linux security is thus not merely about thwarting cyber-attacks—it's about forging and fostering customer relationships, building brand loyalty, and carving a competitive edge in a crowded market.

In essence, *the age of digitization and trust demands a new paradigm: one where Linux security is interwoven with business strategy, customer relations, and brand identity.* Understanding and acting upon this interconnectedness becomes imperative for sustained business success as we navigate this landscape.

WHY SECURITY AND RESILIENCY IS DIFFERENT FOR LINUX

The steps we took in yesteryear no longer match today's challenges' rhythm. The Linux environments of modern enterprises, sprawling and multifaceted, require a renewed choreography, especially when old protection measures miss the beat.

Historically, our gaze in cybersecurity was often rearward, reacting to the echoes of breaches rather than anticipating their approach. This reactive mindset, although prevalent, came with a series of pitfalls. For one, the yawning gap between a breach's occurrence and its eventual detection granted adversaries a generous timeframe. They could wreak havoc, steal valuable data, or lay the groundwork for future incursions. Beyond the immediate technical repercussions, the financial toll of mending post-breach wounds was significant. There were costs tied to reparations, regulatory penalties, and efforts to salvage an organization's reputation. For many, the lingering shadow of a security lapse eroded the hard-earned trust of their customers and stakeholders.

Yet, the challenges continued. Many of our older security tools, forged when infrastructures were more monolithic and static, now strain to protect the dynamic landscapes of today. As enterprises embraced the cloud's expansiveness and the agility of mobile systems, these traditional tools often needed to catch up. They weren't just ill-equipped in their coverage and introduced lags, impeding performance and marring user experiences. The architecture of these tools, sometimes resistant to seamless integrations, posed hurdles in guarding modern, fluid infrastructures.

Adding another layer of complexity was the siloed approach that once characterized our security endeavors - different teams, each ensconced in its operational bubble, deployed unique security measures. While perhaps unintended, this fragmentation obfuscated a holistic view of the threat environment. Disparate security practices, often inconsistent across teams, inadvertently crafted chinks in our armor. These operational chasms made threat detection more arduous and bred inefficiencies, prolonging response times and duplicating efforts. The Linux systems of today, meshed with our ambitions and operations, necessitate a fresh, proactive, and integrated approach to security—one that matches the cadence of our times.

THE STAKEHOLDER LANDSCAPE: A COLLABORATIVE APPROACH

In the organization's cybersecurity realm, every thread and every role has its unique significance. The essence of safeguarding the vast Linux environments isn't about isolated heroes but about a symphony of collaborative efforts, each contributing a crucial note.

At the bedrock of this landscape are the **Infrastructure Engineers**. They're akin to the architects and builders of a medieval fortress, laying down its foundation and ensuring its walls are impenetrable. They labor behind the scenes, designing infrastructures resilient to known threats. Their expertise goes beyond mere construction; they continuously harden servers, ensuring that every access point and gateway stands robust against potential breaches. Their work ensures that even if adversaries approach, the fortress remains unyielding.

Then there are the **Application Developers**, the artisans of this digital realm. They breathe life into the infrastructure with their code, animating the static walls and towers with functionality. Their canvas isn't just about creating; it's about crafting securely. Every line of code they pen can be a gateway for adversaries if not written with security in mind. They need to be well-versed in the language of

vulnerabilities, understanding the profound implications a single oversight can unleash. Beyond creation, they're also the stewards of their craft, ensuring software remains updated and free from known vulnerabilities.

The **Security Practitioners** are guarding this kingdom with a watchful eye. They're ever vigilant, monitoring the digital horizons for signs of threats. Their expertise lies in spotting these threats and swiftly mounting a response, ensuring minimal damage and swift containment. Beyond the immediacies of threat detection and response, they're also the standard-bearers of compliance. They provide that the kingdom operates within the boundaries of laws and regulations, ensuring the realm's reputation remains untarnished.

Each of these roles, while distinct, is interdependent. Like a well-oiled machine, they must operate in harmony for the system to function optimally. Recognizing the contributions of each and fostering a culture of collaboration is pivotal. In the vast expanse of Linux environments, this collective effort, this symphony of skills, stands as the bulwark against the shadows of cyber threats.

THE NEW PARADIGM: PROACTIVE AND RESILIENT LINUX SECURITY

Clinging to static defense measures equates to standing still in a marathon—impractical and ill-advised. Instead, the wave of the future beckons us towards a proactive stance and enduring resilience in Linux security.

Integrative Early-stage Security: Security was often appended towards the tail end of the development process, making it an adjunct rather than an intrinsic component. Now, the narrative is changing. Security is woven into the very fabric of the development lifecycle, beginning at the earliest stages. This approach ensures that applications are conceived with security in mind, guarding against vulnerabilities from their inception and eliminating the need for retrofitted fixes.

Adaptable Automation: The tools designed to protect them must evolve in tandem. Modern security strategies leverage automation, not just for efficiency but also for its adaptability. Organizations can ensure consistent protection by automating routine security tasks while freeing up human resources to focus on more complex issues. Moreover, these tools are designed to be scalable, expanding seamlessly as the infrastructure they safeguard grows.

Real-time Vigilance: Gone are the days of occasional snapshot audits. The contemporary security paradigm acknowledges that threats can emerge at any moment, making continuous monitoring an imperative. Through advanced systems, organizations can keep a perpetual watch on their digital assets, ensuring real-time anomaly detection. This shift facilitates faster responses, narrowing the window of opportunity for potential breaches.

Code-driven Infrastructure: The practice of Infrastructure as Code (IaC) is revolutionizing how we deploy and manage systems. Instead of manual setups, infrastructures are defined and controlled through code. This ensures consistent, repeatable deployments and ushers in an era where infrastructural elements can be automatically vetted for compliance and security postures. This code-driven approach magnifies precision, reduces human error, and introduces an unprecedented level of assurance in system deployments.

Compliance and Security Effectiveness: Modern security distinguishes between mere compliance and true effectiveness. While traditional measures might tick a box by having antivirus software present, it's crucial that such tools are active and optimized. Mere compliance doesn't equate to real-world safety; diligent use and monitoring of these tools fortifies Linux security.

Time to Effectiveness and Level of Effort: A swift time to effectiveness and reduced effort in security measures directly correlate to a higher Return on Investment (ROI). Streamlined processes ensure quicker defensive deployments and minimize resource drain, optimizing cost-efficiency and maximizing the value delivered in Linux security operations.

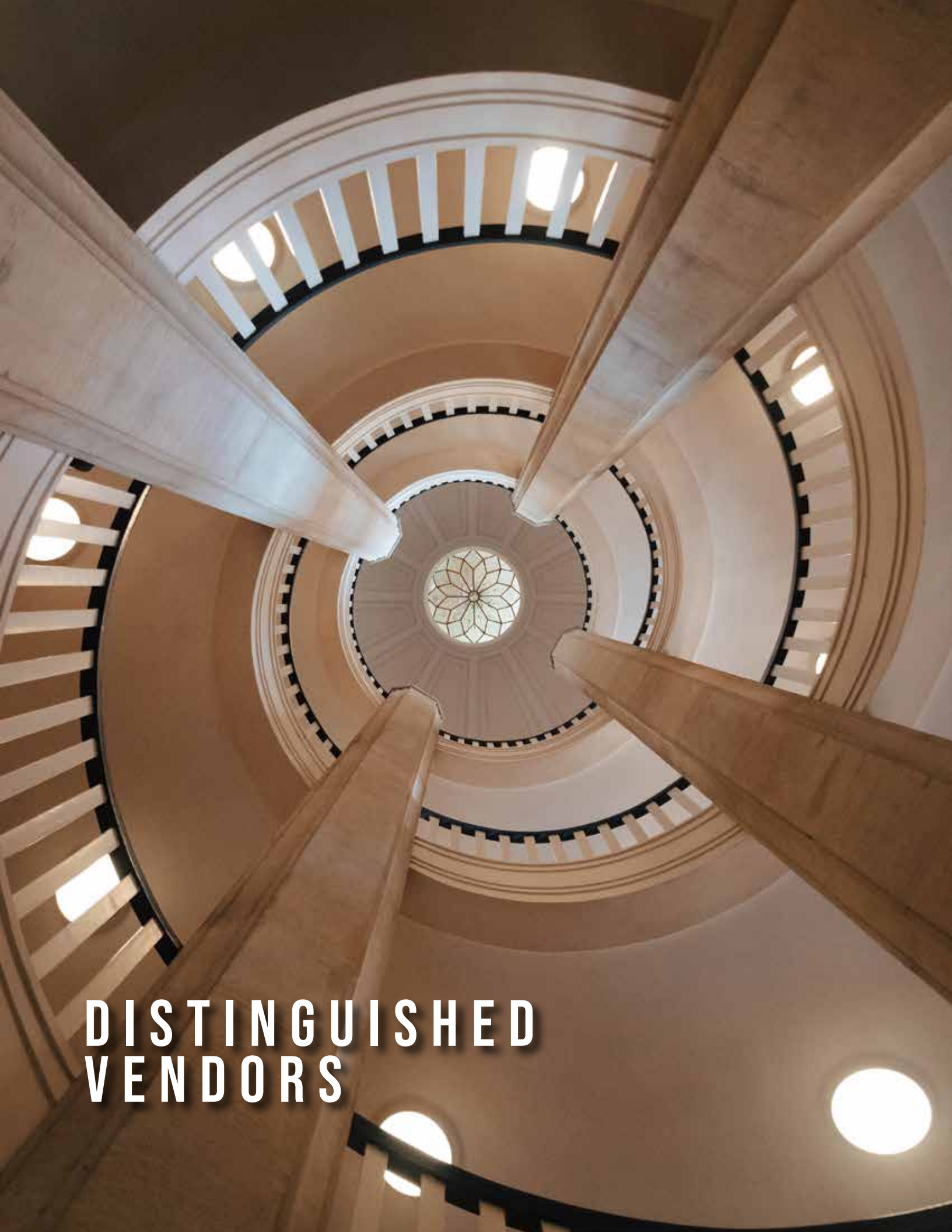
The forward momentum in Linux security is palpable. We're transitioning from reactive stances to positions of anticipation and resilience. The path to a fortified future in Linux security is paved through early-stage integration, automation, relentless vigilance, and a code-centric infrastructure approach.

THE VALI CYBER VALUE PROPOSITION

TAG Cyber believes the landscape of digital operations has broadened remarkably in recent years, diversifying into various environments. Each environment, from public clouds to air-gapped systems, presents challenges and security nuances. Vali Cyber, through its ZeroLock™ platform, has crafted a solution that understands these diverse requirements and offers tailor-made protection for each. Let's delve deeper into each of these coverage areas:

Public Cloud Solutions: As businesses migrate to cloud infrastructure, they often work with an assortment of Bare Metal, VMs, Containers, and Kubernetes. These diverse structures present a myriad of potential vulnerabilities. Vali Cyber's ZeroLock™ has been designed to offer comprehensive protection across this spectrum. Its agility ensures that irrespective of the configuration, your public cloud assets remain shielded from threats.
Private Cloud Environments: Like public clouds, private clouds come with unique challenges, primarily revolving around the controlled access and bespoke configurations they often employ. ZeroLock™ understands this, providing a fully customizable protection framework meticulously crafted for the unique architecture in private cloud settings, ensuring data integrity and system security.
Hybrid Cloud: Merging the realms of public and private clouds, hybrid cloud environments can be intricate. ZeroLock™ shines here, seamlessly bridging security gaps and ensuring that data transition and operation across these combined platforms occur without a hitch, keeping potential vulnerabilities at bay.
On-premises/Private Data Centers: Many organizations still prefer the tangible control of on-site data centers. ZeroLock™ respects this choice, offering robust protection for businesses that keep their data closer to home. This ensures that legacy systems or state-of-the-art data centers remain as secure as their cloud counterparts, regardless of their configuration.
IoT & Edge Devices: The exponential rise of IoT and edge devices presents a complex security challenge, given their varied connectivity statuses. ZeroLock™ steps up, offering unparalleled protection for these devices, ensuring that their security remains uncompromised whether they're continuously online or sporadically connected.
Embedded Systems & Controllers: These form the backbone of many operations, especially in industries like manufacturing or logistics. Any compromise here can be catastrophic. ZeroLock™ recognizes the critical nature of these systems and ensures their protection, guarding the heart of operational integrity.
Air-gapped Environments: One of the most challenging domains in cybersecurity is protecting systems intentionally isolated from external networks. ZeroLock™ has been designed to deliver potent security even in these isolated conditions, ensuring that even the most secluded systems remain immune to breaches.

In essence, Vali Cyber's ZeroLock™ isn't just a security solution—it's a comprehensive protective umbrella, stretching across the vast expanse of modern digital operations, ensuring that no matter where your data resides or how it's configured, it remains safe, secure, and intact.



DISTINGUISHED VENDORS

DISTINGUISHED VENDORS

Q4 2023

Working with cybersecurity vendors is our passion. It's what we do every day. Following is a list of the Distinguished Vendors we've worked with this past three months. They are the cream of the crop in their area—and we can vouch for their expertise. While we never create quadrants or waves that rank and sort vendors (which is ridiculous), we are 100% eager to celebrate good technology and solutions when we find them. And the vendors below certainly have met that criteria.

Arctic Security

Arctic Security is a pioneering force in cybersecurity, dedicated to empowering defenders by identifying threats before they harm a company's business. We deliver reliable data on early signs of breaches and vulnerabilities, facilitating proactive incident prevention. Our affordable, automated solutions integrate seamlessly, saving companies time and resources.

Amenaza®

TECHNOLOGIES LIMITED

Amenaza Technologies Ltd. is a leading threat analysis and risk assessment solutions provider. With its flagship product, Secure*ITree*®, the company assists organizations in identifying potential vulnerabilities, analyzing threat scenarios, and optimizing security countermeasures. Founded in 1998, Amenaza Technologies is headquartered in Calgary, Canada, serving diverse global clients.

CLOUD RANGE

Cloud Range, the leading cyber range-as-a-service, measurably decreases exposure to cyber risk and overcomes the staggering skills gap by preparing security teams to defend against complex attacks through a customized, full-service, simulation-based cyber attack training program, including live-fire team simulations, IT/OT/IoT environments, skill development labs, assessments, reporting, and more.

Island

Island is the browser designed for the enterprise that makes work fluid yet fundamentally secure. With the core needs of the enterprise embedded in the browser itself, Island enables organizations to shape how anyone, anywhere, works with their information while delivering the Chromium-based browser experience users expect: Island, The Enterprise Browser.

TAG CYBER DISTINGUISHED VENDORS

2023

Nudge Security, founded in 2021 by Jaime Blasco and Russell Spitler, aids distributed organizations in effectively managing SaaS security and governance. Recognized by CSO Magazine as a "Cybersecurity startup to watch" and an SC Awards finalist for "Most promising early-stage startup," Nudge champions employee-centric security solutions. Discover more at www.nudgesecurity.com or follow them on Twitter and LinkedIn.

Panorays is a rapidly growing third-party security risk management software provider offered as a SaaS-based platform. The company serves enterprise and mid-market customers primarily in North America, the UK, and the EU. Top-tier banking, insurance, financial services, and healthcare organizations have embraced the platform.

PlainID Inc., a leading Authorization-as-a-Service provider, leverages Policy Based Access Control (PBAC) to simplify authorization management, enabling organizations to create, enforce, and manage policies enterprise-wide. Firms meet user journey demands through secure identity-to-asset connections, implementing zero-trust architectures, and enhancing data security. The PlainID Authorization Platform facilitates business growth by integrating technologies with advanced authorization features.

RapidFort.com is the pioneering Software Attack Surface Management platform (SASM), offering comprehensive runtime and build-time tool suites. Our cutting-edge solutions empower organizations to scan, analyze, and fortify modern software, ensuring enhanced security and resilience while safeguarding software from potential vulnerabilities.

RedSeal delivers actionable insights to close defensive gaps across the entire network, on-premises, and in the cloud. Hundreds of Fortune 1000 companies and over 75 government agencies, including five branches of the U.S. military, depend on RedSeal for exceptionally secure environments. Visit www.redseal.net to learn more.

SafeBreach is a cybersecurity company headquartered in Sunnyvale, California. Founded in 2014, it offers a comprehensive platform for simulating and optimizing security postures. SafeBreach enables organizations to proactively identify and mitigate security risks, providing valuable insights to enhance their overall cybersecurity resilience. Their innovative approach helps safeguard businesses from emerging threats.

TAG CYBER DISTINGUISHED VENDORS

2023

SecureCo provides network security solutions protected by stealth and obfuscation. Our innovative approach shields networks, APIs, and cloud connections from reconnaissance, exploitation, and breach. Trusted for the most demanding commercial and government cybersecurity applications, we deliver high-performance, exceptionally secure endpoint and data transit protection, reducing attack surface, vulnerability, and administrative overhead.

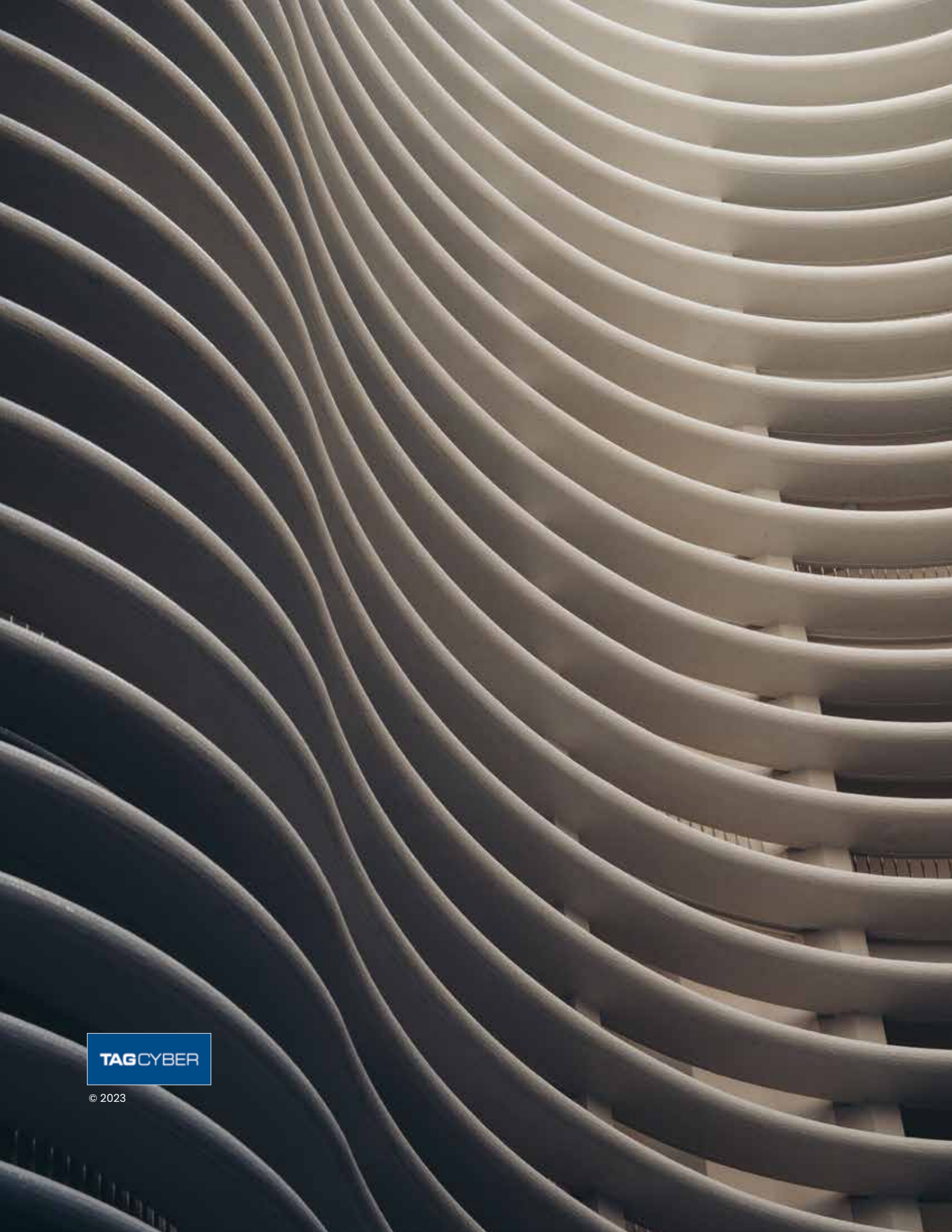
Semperis is a pioneering cybersecurity company providing enterprise-level identity protection solutions. Their Identity Resiliency Platform offers comprehensive protection for Active Directory (AD) and Azure AD, ensuring operational resilience against cyber threats. Semperis also provides automated remediation, swift recovery tools, and dedicated incident response services, making them a trusted cybersecurity partner.

ShardSecure is a cybersecurity company that specializes in Microsharding technology. Their revolutionary solution disassembles data, distributes the shards across multiple clouds, and renders them useless in isolation. By making data breaches unattractive and unrewarding, ShardSecure provides organizations with unparalleled security. The company, founded in 2018, has its headquarters in New York, USA.

Established in 2020, Vali Cyber, Inc. is dedicated to addressing Linux security needs. We've developed ZeroLock™, a security platform based on DARPA-funded MIT and CMU research. It offers comprehensive lockdown and superior threat detection, all with minimal resource consumption compared to legacy Linux security tools.

Vectra AI is the leader in hybrid attack detection, investigation, and response. The Vectra AIPlatform delivers integrated signals across the entire hybrid cloud attack surface in a single solution. Organizations worldwide rely on the Vectra AI Platform and MDR services to power their XDR strategy.

Votiro is a Zero Trust Content Security company that detects, disarms, and analyzes billions of files between organizations, their employees, and the customers that rely on them. Votiro is an open API platform that allows teams to receive safe, fully functional files without slowing down business.



TAGCYBER