Insigniam QUARTERLY®

DISRUPTIVE FORCES & CRITICAL SUCCESS FACTORS | CYBERSECURITY

Phishing for Trouble

Are you prepared to defend your corporate estate from next-gen cyber threats?

BY **JOE HUBBACK**
SUPPORTING RESEARCH BY **JON BALL**

ADOBE STOCK

The global cybersecurity industry has expanded to an immense scale, driven by the escalating frequency and severity of cyber threats. In 2024, the average cost of an enterprise data breach reached a record $4.88 million (USD), reflecting the increasingly expensive impact of cyberattacks on businesses. Human error plays a significant role, contributing to 88% of cybersecurity breaches, which take an average of 194 days to be identified—and 292 days to contain.

Making matters worse, cyber fatigue—where companies become apathetic to proactively defending against attacks—is rising, further exacerbating vulnerability to threats. Cisco reports that 42% of companies surveyed are currently experiencing some form of cyber fatigue. Yet, according to Check Point, this comes at a time when there is a 30% year-over-year increase in cyber attacks globally, reaching 1,636 attacks per organization per week. Latin America, Africa, and Europe showed the largest increases in cyber attacks in Q2 2024, at 53%, 37%, and 35% increases, year over-year, respectively.

Enterprises notwithstanding, consumers are also at significant risk. In 2022, over 1.1 million reports of identity theft were filed with the U.S. Federal Trade Commission, yet a staggering 64% of Americans have never checked if they were impacted by a data breach. Recently, in June 2024, over 560 million Ticketmaster customers had their information stolen in a data breach. And in 2023, an AT&T breach exposed approximately 9 million customers' personal details.

Compounding the problem further, the International Information Systems Security Certification Consortium reports that 70% of cybersecurity professionals say their organizations are understaffed, hampering their ability to be proactive. Additionally, the likelihood of prosecuting cybercriminals remains astonishingly low, estimated at just 0.05% by the World Economic Forum. To navigate growing challenges, businesses must understand and address the key disruptive forces shaping the cybersecurity industry over the next five years, influencing their ability to mitigate risks and protect their digital estates.

Based on research and insights from the cybersecurity industry, the top five disruptive forces impacting executives' and enterprises ability to respond to—and mitigate—digital threats include:

11%

High-profile attacks such as the SolarWinds breach, which affected over 18,000 systems worldwide, cost companies an average of 11% of their annual revenue. The attack exposed how deeply interconnected businesses are with their technology providers, and how ripple effects can impact numerous organizations globally.

1 Supply Chain Vulnerabilities

One of the most significant disruptors in the cybersecurity landscape, statistics regarding supply chain vulnerabilities indicate that 91% of organizations faced a software supply chain attack last year. High-profile attacks such as the SolarWinds breach, which affected over 18,000 systems worldwide, cost companies an average of 11% of their annual revenue. The attack exposed how deeply interconnected businesses are with their technology providers, and how ripple effects can impact numerous organizations globally.

In the case of SolarWinds, hackers inserted malicious code into a routine software update, enabling them to infiltrate the systems of countless businesses and government agencies. This event served as a wake-up call for executives to recognize that no company is an island in today's digital ecosystem.

The challenge for executives is understanding that their cyber risk extends beyond their own internal defenses. Every vendor, partner, or third-party provider they rely on represents a potential entry point for cyber attackers. Many companies have limited visibility into their extended supply chain, which makes it difficult to assess the cybersecurity posture of every partner. This blind spot can level organizations.

2 An Evolving Threat Landscape

According to various sources, there are around 2,200 cyber attacks per day, or one attack every 39 seconds. Not only are the attacks more frequent, but they are also more sophisticated in nature.

ISTOCK

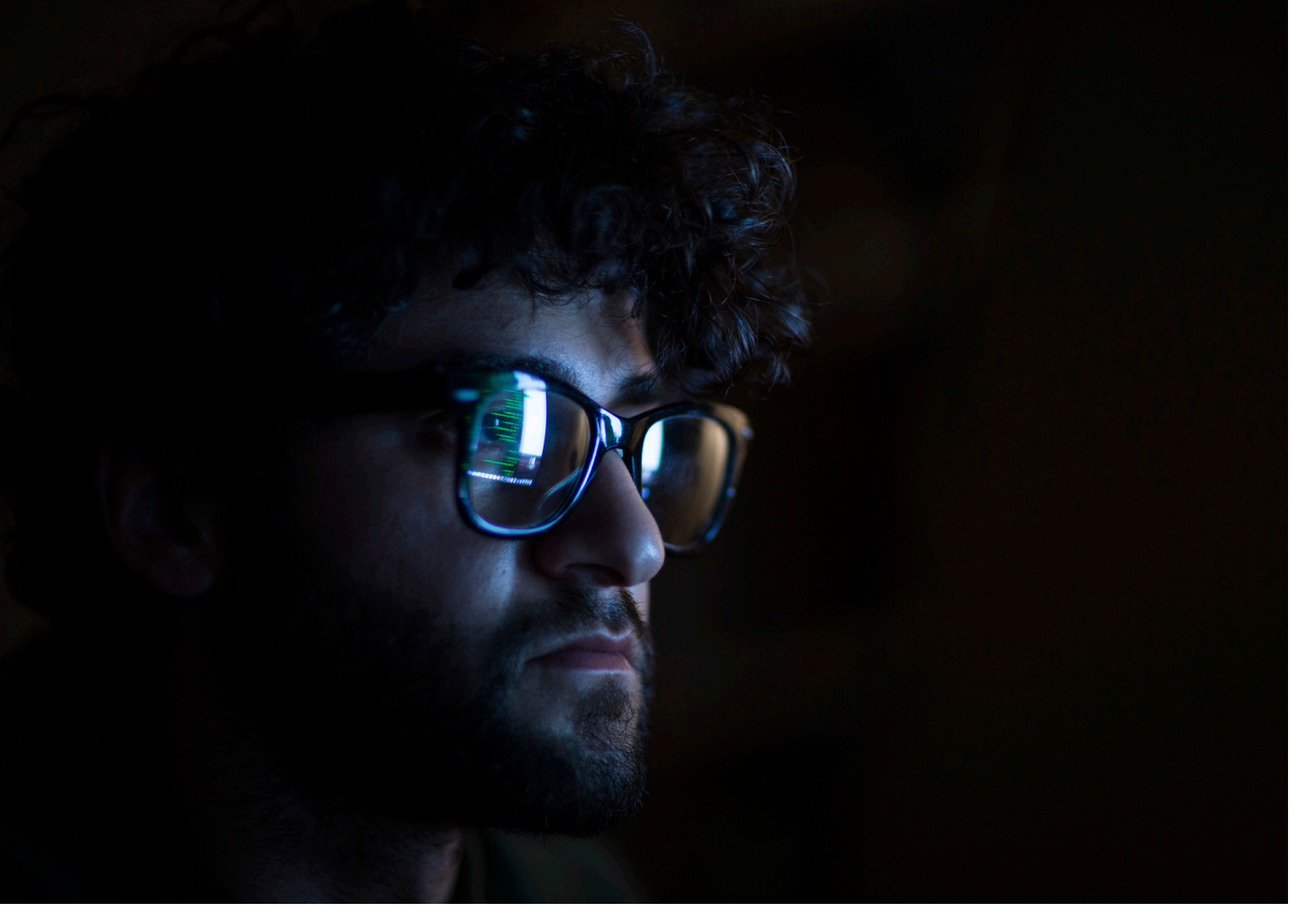
No longer limited to simple hacking attempts, today's attackers range from opportunistic criminals seeking financial gain to highly sophisticated nation-state actors with strategic political motives.

This diversity in threat actors makes it increasingly difficult for organizations to predict where attacks might come from and what assets may be at risk.

For executives, the challenge lies in understanding who might target their organization—and for what purpose. Cybercriminals may be after sensitive customer data, intellectual property, or financial information, while nation-state actors may seek to disrupt operations for geopolitical reasons. Understanding the motivation behind these attacks is crucial for developing a robust defense strategy, wherein executives can prioritize their cybersecurity efforts and allocate resources effectively.

Moreover, the rapid advancement of technology also amplifies the risks associated with the evolving threat landscape, including the proliferation of AI-powered cyber threats. As companies implement AI systems, attackers will increasingly use AI to craft more sophisticated attacks, such as AI-generated phishing and autonomous malware.

Malware, Everywhere
In 2022, over 1.1 million reports of identity theft were filed with the U.S. Federal Trade Commission, yet a staggering 64% of Americans have never checked if they were impacted by a data breach.



Detection Perfection
Experts say cybersecurity systems and protocols must evolve continuously to address the shifting threat landscape, from new malware strains to increasingly sophisticated phishing tactics.

3 Balancing Integration and Independence

While it's essential for business units to be well-integrated and understand their cyber risks, it's equally important for companies to avoid becoming overly reliant on a single provider. This reliance can create vulnerabilities that could be catastrophic if that provider suffers a failure or a cyber attack.

The recent CrowdStrike incident in July 2024 is a prime example of how the compromise of one vendor can affect an entire ecosystem, disrupting operations for thousands of businesses across various industries, when a faulty update to CrowdStrike Falcon Sensor software caused widespread disruptions across organizations globally. The update, which was intended for Windows systems, led to severe outages, affecting approximately 8.5 million devices worldwide. Key sectors such as healthcare, banking, and airlines were particularly impacted. Customers experienced business interruptions, with some facing extended downtime while systems were manually restored. The issue underscored the critical risk of over-reliance on a single provider and the cascading effects of such disruptions across interconnected industries.

Building external independence involves leveraging multiple vendors and implementing backup systems that can quickly take over in case of an emergency. This could include having various providers for key services, such as cybersecurity tools or cloud platforms, and using varied infrastructure across different regions.

Additionally, a hybrid approach that mixes in-house solutions with external providers can help companies maintain more control over their critical systems while still benefiting from the innovation of third-party vendors.

4 A Lack of Cyber Resiliency

Many organizations mistakenly view cybersecurity as a one-time project, treating it like a task with a clear start and finish. The idea of a "set it and forget it" approach is outdated and dangerous, leaving companies vulnerable to breaches.

ISTOCK

Cybersecurity systems and protocols must evolve continuously to address the shifting threat landscape, from new malware strains to increasingly sophisticated phishing tactics. Businesses that fail to embed cybersecurity into their daily operations face higher risks of attacks. Resilience is not just about prevention, but about recovery. In the event of an attack, businesses need robust systems to mitigate damage and bounce back quickly. This involves having clear incident response plans and ensuring all stakeholders know their role in protecting the company.

5 Evolving Regulatory Landscape and Compliance Risks

As digital transformation accelerates, governments and regulatory bodies worldwide are enacting stricter data privacy and security laws. Laws such as the General Data Protection Regulation (GDPR) in Europe and the California Consumer Privacy Act (CCPA) in the U.S. are setting new standards for how companies must handle and protect sensitive data.

The regulatory tsunami is not just a factor in the US and EU, but also on six different continents and in seventy-six countries, which sits on top of existing AI laws in 127 countries that are already in place, having been enacted since 2016. From a regulatory perspective, board directors and corporate governors could be held personally accountable if their company's AI-enabled platforms go awry, placing them squarely in regulators' cross-hairs as legislation becomes codified.

Non-compliance with these regulations can have severe financial consequences. For instance, companies found violating GDPR can face fines of up to 4% of their global annual revenue, a penalty that has already been imposed on major corporations like Meta. Similarly, in the U.S., the California Attorney General has been aggressively enforcing CCPA, which can result in significant fines for data breaches or failures to properly notify consumers.

Failure to meet these regulatory expectations not only risks hefty fines but also operational disruptions, as regulators may impose restrictions on business activities.

Critical Success Factors

In a 1984 Sloan Management Review article titled, "An Assessment of Critical Success Factors," A.C. Boynlon and R.W. Zmud wrote:

"Critical success factors [CSFs] are those few things that must go well to ensure success for a manager or an organization, and therefore, they represent those managerial or enterprise areas that must be given special and continual attention to bring about high performance. CSFs include issues vital to an organization's current operating activities and to its future success."

For global executives and enterprises to survive—and thrive—amid increasingly sophisticated cyberthreats over the next five years, the following critical success factors will be key:

Focus on Risk Transparency

To ensure cybersecurity risk transparency in large-scale global enterprises, executives must follow a structured approach that addresses both current threats and the evolving risk landscape.

The first step is to conduct a thorough risk assessment, which involves identifying and categorizing potential cyber risks specific to the business, such as operational disruptions due to cyber attacks or confidential data loss due to cyber theft. Each type of threat poses different challenges, and understanding the motives behind them is essential for crafting tailored defenses. Companies should start by identifying and prioritizing critical assets and then considering the potential threats against them that, together, constitute their priority risks.

The next step is implementing risk monitoring tools that provide continuous visibility into potential vulnerabilities. Furthermore, real-time monitoring is essential to maintaining transparency and allowing for a rapid response to emerging threats. With these tools in place, executives can quickly detect anomalies or breaches and act before they escalate. Generating actionable insights from the collected data is crucial for informed decision-making. These insights help companies allocate resources effectively, ensuring the most significant risks are addressed first. Strategic resource allocation allows organizations to focus on high-risk areas while avoiding unnecessary spending in less critical sectors.

The recent CrowdStrike incident in July 2024 is a prime example of how the compromise of one vendor can affect an entire ecosystem, disrupting operations for thousands of businesses across various industries.

Finally, cybersecurity strategies must be reviewed and adapted continuously. Regular audits and reassessments ensure that the organization's defenses evolve alongside emerging threats, as the dynamic nature of cyber risks.

Build Resilience Across the Enterprise

Building cybersecurity resilience in large-scale global enterprises requires a strategic and methodical approach, and the first step is to ensure internal integration across all business units. Each department must align and coordinate its cybersecurity efforts, developing clear communication channels that facilitate a rapid response to any threats. Organizations with strong internal coordination are better equipped to manage crises, as they can leverage collective resources and expertise to mitigate risks across various departments.

External resilience is equally important, and executives must avoid over-reliance on a single provider, as illustrated in the CrowdStrike example. To engrain enterprise resilience, companies should implement decentralized backup systems.

This is why maintaining cloud-based and offline backups is essential for ensuring continuity during an attack or system failure, and these backups allow for quicker restoration of operations, minimizing downtime and the impact on business functions. Fail-safe systems should be regularly tested to ensure they work when needed, which includes conducting regular simulations and drills to identify any weaknesses in the recovery process.

Finally, resilience is not static, and companies must continuously adapt their cybersecurity strategies. Emerging threats require constant reassessment and updates to internal processes and technologies.

Don't Neglect Continuous Iteration & Adaptation

To create a system of continuous iteration and adaptation for cybersecurity in large-scale global enterprises, the first step is to establish a dynamic cybersecurity framework that can adapt to new threats and technological advancements.

Cyber threats are constantly evolving, so organizations must have flexible frameworks that allow for quick iterations and the integration of new tools and policies as needed. This adaptability is essential for maintaining an effective defense in an increasingly complex threat landscape.

Next, routine processes should be enacted across all platforms and devices, which are critical to maintaining security (i.e., patching and system updates are classic issues that still cause problems). Automated systems can help ensure that updates are applied consistently, keeping the organization's digital infrastructure secure and up to date. This proactive approach closes security gaps that could otherwise be exploited.

Additionally, continuous security testing is essential for identifying weaknesses early. Regular penetration testing, vulnerability scans, and security audits allow businesses to pinpoint and address potential vulnerabilities before they are exploited.

Finally, real-time monitoring systems, enhanced by AI and data analytics, allow organizations to detect potential risks and predict future attack patterns, which enables faster response times and reduces the potential impact of cyberattacks.

Infuse Cyber Awareness Across the Organization

To build cyber awareness across the enterprise, leaders must establish a comprehensive cybersecurity policy that clearly outlines security protocols and expectations. This policy, or "north star," should be accessible to everyone in the company, ensuring that cybersecurity is recognized as a shared responsibility.

Cybersecurity training should also be embedded in the onboarding process for new employees. This ensures that from day one, employees are equipped with the knowledge to protect against threats like phishing, identity theft, and data breaches.

Additionally, regular, ongoing training is equally critical, as cyber threats are continuously evolving. Employees should be kept up to date on the latest threats and defenses through interactive workshops or online modules, ensuring they remain vigilant and prepared for new risks.

Lastly, executives should foster a culture of cyber awareness by integrating security into daily operations and communications. Using regular team meetings, internal newsletters, and leadership messages can encourage open conversations about cyber risks. Continuous evaluation of the program ensures that it evolves alongside emerging threats, maintaining its effectiveness over time.

Get Serious About Cybersecurity Budgeting

Creating an effective cybersecurity budget requires executives to assess the unique cybersecurity needs across their organization and identify specific threats and vulnerabilities each department or business unit faces—from protecting intellectual property to safeguarding customer data. A one-size-fits-all approach to cybersecurity budgeting is inefficient; by understanding the distinct risks faced by different areas of the organization, executives can ensure that the budget is distributed appropriately.

Another key step is adopting a risk-based budgeting approach. Cybersecurity investments should be proportionate to the financial and operational risks the organization faces. Critical assets, such as customer data or high-value intellectual property, should receive a larger share of the budget to ensure they are adequately protected. This strategy helps avoid overspending on low-risk areas while ensuring that the most vulnerable parts of the organization are fully secured.

4%

Percentage of their annual revenue that companies can be fined for violating GDPR regulations, already imposed can on major corporations like Meta.

Finally, by regularly evaluating the effectiveness of their cybersecurity tools and policies, companies can ensure that their spending is delivering ROI. Regular reviews and adjustments to the budget can also ensure that the cybersecurity strategy evolves to meet new challenges, creating a flexible and effective financial plan for cybersecurity.

Take Five

In the face of mounting cyber threats and challenges, it is not just the technology, but the strategy that sets apart those who thrive from those who falter. Companies that weave resilience into their very DNA through risk transparency, continuous adaptation, diversified vendor strategies, and rigorous budgeting—are best positioned to overcome the looming threats.

Simply put, it's not enough to simply build walls—businesses must craft networks of trust, transparency, and readiness across their entire ecosystem. By making cybersecurity a collective effort that spans departments, supply chains, and even regulatory frameworks, they can stay ahead of the attackers. Yet, it requires continuous attention, and that's where many fall short. Executives who view cybersecurity as a one-time checkbox will be left scrambling in the wake of the next breach. Those who adapt, iterate, and invest in long-term resilience will not only weather the storm they'll set the standard for how to do business in the digital age. The clock is ticking, and the future belongs to the prepared. **IQ**

EXECUTIVE PERSPECTIVE: INFORMATION SECURITY

BO FALK

Regional Head of Information Security
ISS A/S

Information security is a foundational concern that should be baked into the DNA of every enterprise around the globe—but what will be required of those working in cyber security over the next five years? To better anticipate those needs and challenges, *IQ* spoke with Bo Falk, regional head of information security (APAC) at ISS A/S, a leading facility management services company founded in Copenhagen, Denmark. Prior to his current role, Mr. Falk served as global head of business information security and business information security officer at ISS A/S. Additionally, Mr. Falk holds a cybersecurity certification from the University of Cambridge's Judge Business School.

IQ: What are the top challenges executives and enterprises within the cybersecurity industry must contend with over the next five years, and why?

Mr. Falk: The biggest challenge is the sheer pace of change. One day everything seems stable, and the next day, new technologies like quantum computing and AI are introduced, fundamentally altering the landscape. As a business, we need to be able to adapt quickly to these shifts and remain flexible in our approach to meet market demands. With this rapid change comes the challenge of keeping up. For example, when AI was first introduced, a flood of so-called experts emerged overnight, providing sometimes conflicting information or advice. This highlights how critical it is to quickly and accurately build an understanding of these technologies within our organizations, and how they will impact or change your risk landscape.

The pace of change is pushing businesses to innovate, but we must ensure we have the necessary infrastructure and security controls in place. The business side is eager to implement the latest and greatest, so we need the agility to support these initiatives securely. A "plug and play" architecture and security model is becoming essential, allowing us to swiftly adapt to the businesses demands without compromising safety and security.

A big part of my role is helping the business understand that security is more than just technology—it's a strategic component of business. Information security must align with business requirements, not hinder them. It's about showing how security supports the business as an enabler of business success.

***IQ*: Do you have a sense of how companies and leaders in the cybersecurity space are currently adapting their strategies to manage and mitigate these risks?**

Mr. Falk: There's definitely a shift in mentality. Historically, information security was often an afterthought, primarily driven by compliance. But we're seeing businesses that adopt security early on realizing that they can lower costs in the long run. I'm now being included much earlier in the process—right from the ideation phase—which allows me to shape security from the outset.

Think of it like building a house: if you wait until the walls and floors are up before planning the electrical wiring or plumbing, it becomes much more difficult, complicated, and expensive to retrofit everything. The same applies to cybersecurity. When security is integrated early, it's more efficient, cost effective, and less disruptive. We can't afford to implement security last minute or rush the process. It needs to be embedded from the start to be truly effective and cost effective.

***IQ*: Despite the challenges, what are the most promising opportunities for growth within the cybersecurity sector over the next five years? Is there a potential game-changer?**

Mr. Falk: One of the biggest opportunities lies in the alignment between business and security. Fifteen years ago, we were often seen as the "no" department, the ones who slowed things down. But today, there is a shift to that perception, bringing forward our value proposition as trusted, secure partners for our clients. Our reputation is increasingly tied to how well we handle security and resilience, and that's a powerful differentiator. By investing in information security, we can actually help businesses grow their capabilities while safeguarding their operations.

Building and maintaining trust and a brands reputation through security. The real game-changer here is leveraging security as a core value proposition, making it a business enabler rather than just a cost center. The World Economic Forum has noted that many executives now see information security as a competitive advantage, not just a necessary expense.

For clients, trust and reputation are everything. If we can demonstrate that security is one of our strengths, it becomes a feather in our cap—something we can actively sell and build on in the market.

PHOTO COURTESY OF LINKEDIN

***IQ*: What attributes will be required of leaders and executives in cybersecurity to ensure their organizations survive and thrive over the next five years?**

Mr. Falk: The most impactful attribute for leaders is the ability to champion information security. Executives need to understand cybersecurity at a strategic level—its objectives and the long-term benefits it brings to the organization. They must communicate the importance of security, as people naturally follow the example set by their leaders. If executives aren't comfortable discussing cybersecurity, they won't inspire confidence in their teams or within the organization.

Leaders need a foundation of knowledge, enabling them to lead effectively and share their vision with others. Passion is infectious, so we need to be able to speak about information security with confidence and passion.

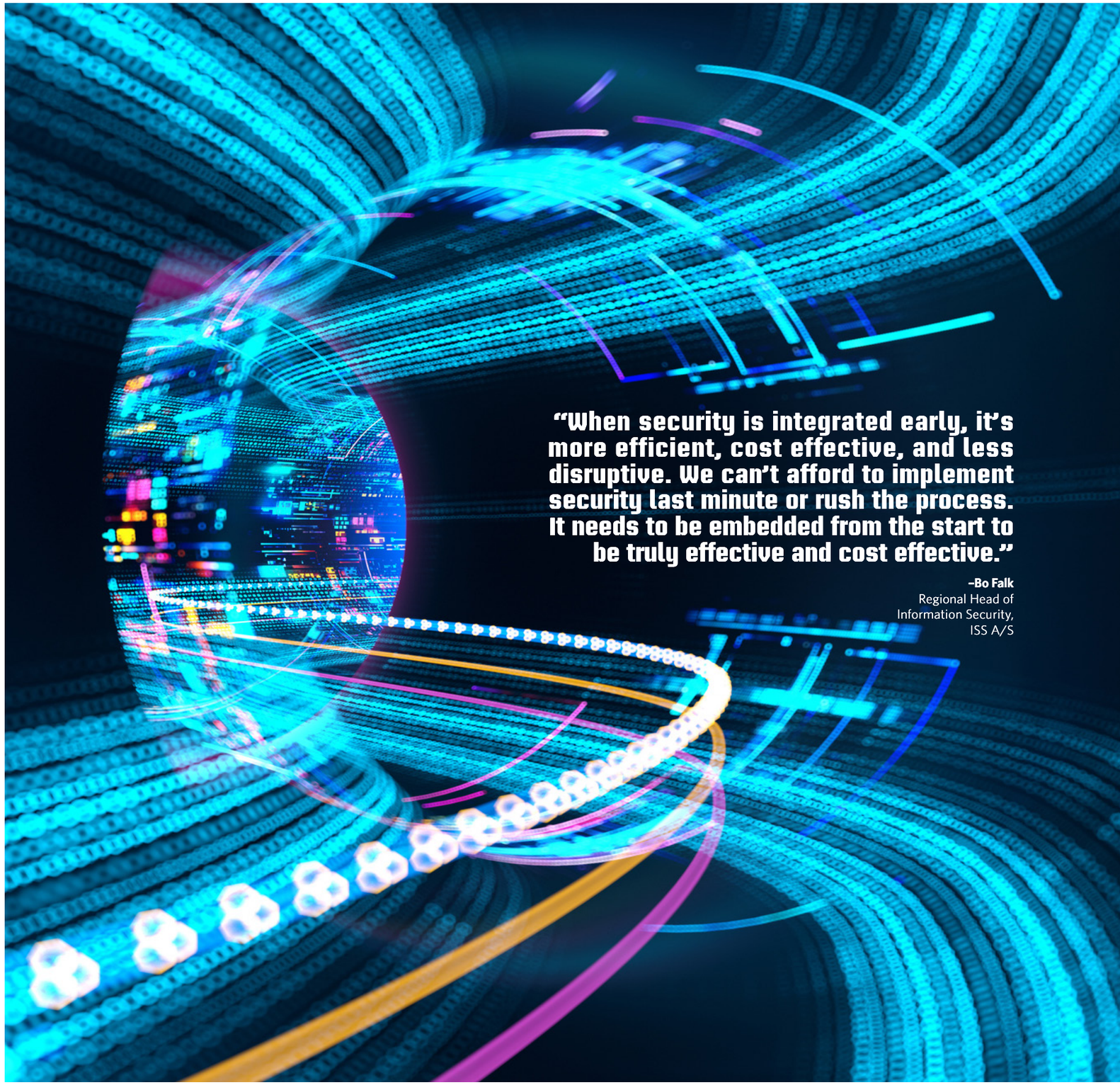
Leaders must bridge that gap, translating technical cybersecurity concepts into clear, actionable insights for broader strategic decisions. This not only improves internal understanding but ensures cybersecurity becomes embedded in the organization's overall growth strategy.

IQ: Lastly, how critical is maintaining trust in the cybersecurity industry, and what proactive steps should executives take to ensure they protect their brand's reputation and financial stability?

Bo Falk: One of the most important aspects of information security is trust. We build, hold, and maintain trust in our business, and that trust is fragile. An incident can easily tarnish a brand, whether you're in B2B or B2C. Once people lose trust in your brand, it's incredibly difficult to regain. No executive wants to be at the helm when things go wrong—it's always easier to invest in prevention than recovery.

If trust is lost due to a cybersecurity failure, not only will it impact the company's reputation, but it could also have serious financial consequences, like a drop in share price. Businesses have suffered 10% to 20% drops in share prices overnight, due to poor information security response and practices.

My advice is to not wait for something to go wrong before taking action. Instead, put in the work now, invest in proactive security measures, and safeguard that trust. Doing so will save you from greater losses down the line, both in reputation and in finances. **IQ**



ISTOCK