TAG
2024
Security Annual
SPECIAL REPRINT EDITION

EXPLORING CUTTING-EDGE SECURITY AUTOMATION

AN INTERVIEW WITH CODY CORNELL,
CO-FOUNDER & CHIEF STRATEGY OFFICER, SWIMLANE

THE STATES OF CYBERSECURITY

REDEFINING CYBERSECURITY: FROM DEFENSIVE MEASURES TO A STRATEGIC BUSINESS STRATEGY

TAG DISTINGUISHED VENDOR
SWIMLANE

The need to reduce cyber risk has never been greater, and Swimlane has demonstrated excellence in this regard. The TAG analysts have selected Swimlane, Inc. as a 2024 Distinguished Vendor, and such an award is based on merit. Enterprise teams using Swimlane's platform will experience world-class risk reduction—and nothing is more important in enterprise security today.

The Editors,
TAG Security Annual
www.tag-infosphere.com

REPRINTED FROM THE TAG SECURITY ANNUAL

AN INTERVIEW WITH CODY CORNELL, CO-FOUNDER & CHIEF STRATEGY OFFICER, SWIMLANE

EXPLORING CUTTING-EDGE SECURITY AUTOMATION

The security operation center (SOC) has become a functional component of every enterprise, serving as the main coordinating point for data analysis, incident review, security monitoring, threat hunting, and many other tasks. To provide for automation in this context, teams must select the best available industry partners.

Cybersecurity company **Swimlane** has been a leader in supporting automation in the modern SOC for many years. Their low-code security automation platform extends beyond security orchestration, automation, and response (SOAR), leveraging generative AI to improve security workflows in or beyond the SOC. The interview that follows outlines their evolving approach.

TAG: Tell us a bit about the evolution of your platform and its current set of offerings.

SWIMLANE: When building our platform, we focused on scalability, composability, and flexibility. Unlike other SOAR companies (like Phantom and Demisto) that built pre-set SOC playbooks, we aimed to create a flexible automation engine. As the world's most capable security automation engine, we can integrate and automate anything, becoming the system of record for any security use case or function.

Turbine, our low-code security automation platform, is known for being the world's fastest and most scalable security automation platform, executing over 25 million daily actions—ten times faster than any other platform, provider, or technology. The cloud-native platform has the future of SecOps in mind and can adapt to constantly evolving environments, exceeding the modern SOC's pace of change.

This year, we **announced** Canvas and Hero Artificial Intelligence (AI), our **new Turbine innovations** empowering security teams to build automation in seconds with limitless integrations and dramatic time and resource savings. **Turbine Canvas** unveils the true power of low-code—it democratizes automation and leverages modular and reusable programming components so users can build playbooks with intuitive, ultra-simple visual interfaces.

Hero AI enables customers to be generative AI applications in the Swimlane Turbine platform. Its potent combination of human and machine intelligence optimizes SecOps workflows and maximizes analyst productivity and return on investment. These transformational innovations now make Swimlane Turbine the triple threat of automation, GenAI, and low-code, solving the most challenging problems across the entire security organization.

TAG: What is the role of automation in the SOC, and how does your platform support this goal?

SWIMLANE: Security teams face a shortage of qualified staff, an overwhelming volume of alerts, and underutilized security tools that don't work together. The result is wasted resources and increased vulnerability to evolving threats. Automation is the solution to this critical gap, providing security teams with the necessary tools to protect their organizations fully.

Turbine, our low-code security automation platform, is known for being the world's fastest and most scalable security automation platform.

Recognizing this urgent need, we revolutionized our Turbine low-code automation platform with advancements that strengthen security teams by connecting them, their telemetry, and technology through a human-centric AI and automation building experience. Turbine's automation solutions can ease the burden on security teams, enabling them to tackle more complex threats and deliver greater value to the organization.

TAG: Is AI a vital component of the automated support you provide for customers?

SWIMLANE: Automation and AI have the power to be the ultimate human enabler, but neither will entirely replace the value of the human mind. Instead, AI-enabled features can empower humans to make faster and more effective decisions.

While AI holds immense promise in SecOps, its implementation hinges on experienced human oversight. The talent shortage in cybersecurity creates a vulnerability gap where even advanced AI faces the limitation of bias and unforeseen scenarios. Human expertise is crucial for responsible use, issue identification, and critical decision-making. Like automation, AI in SecOps should involve close human collaboration.

Security automation serves as a valuable foundation for responsible AI adoption. Like the "human-in-the-loop" approach, automation strategies emphasize human involvement in critical decision-making, which aligns with the need for human oversight in AI-powered security. By automating threat detection and log analysis, security professionals can focus on complex situations and strategic decisions where human judgment is irreplaceable.

TAG: What do you see as the interaction between SOC analysts and the tools they use to process and analyze data?

SWIMLANE: SOC analysts face data overload from disparate security tools, which hinders threat visibility and forces analysts to constantly task-switch across tools, browser tabs, and disjointed views. Automation centralizes and enriches information automatically, making teams more effective and efficient.

Collaboration is key. Analysts act as guides, identifying data feeds and defining rules for automation to prioritize threat investigation and response. Automation eliminates irrelevant data and highlights suspicious activity, freeing analysts to investigate high-priority alerts, leverage automation for deeper analysis, and build feedback loops to improve their tools.

The interaction is cyclical. Analyst insights are fed back into the tools, continuously improving threat detection and response. Automation isn't a replacement—it's a force multiplier that empowers analysts to become strategic decision-makers focused on the most critical cybersecurity tasks.

TAG: Any predictions regarding automated security in the SOC for the coming years?

SWIMLANE: AI and security automation are easing the cybersecurity talent shortage by accelerating the onboarding of security analysts. At Swimlane, we process billions of signals for our customers and estimate that our automation does the work of several thousand security analysts. SOC teams will look for ways to do more with less in the coming year—AI and automation will help address this challenge by reducing manual tasks and streamlining workflows. Automating repetitive, time-consuming tasks frees employees to focus on more strategic and creative activities. In addition, powerful AI models can be trained to aid security analysts, further improving this massive efficiency gain.

AI will be a true enabler for security teams by ensuring they are well-equipped to analyze and generate playbooks that build off the team's past actions for specific investigations. By leveraging generative AI for investigations, this tool will ultimately become a readily available knowledge source for security analysts and become critical to shortening the onboarding time for security teams with high attrition rates.

THE STATES OF CYBERSECURITY

JOANNA BURKEY, SENIOR ANALYST, TAG

To get a real picture of the state of any given topic, it's common best practice to ask the experts. And there certainly are plenty of experts in cybersecurity to ask these days. In fact, just reference the other articles in this publication. But what about topics that are so far-reaching, so broad that they have a consistent and direct effect on an audience far larger than only experts? Cybersecurity is, without a doubt, one of these topics. It is difficult if not impossible to find anyone that is not in some way affected by this topic, so let's look at the state of cybersecurity from a few additional points of view.

We hear frequently that "perception is reality." And for three groups of people in particular, their perception of cybersecurity—and more importantly, their reactions in response—have a tangible and daily impact. These groups are: company employees, company officers and directors, and everyday citizens. The understanding of cybersecurity, and how understanding guides the actions of each of these groups,

can have an outsize effect on the success or failure of cyberattacks that are in motion at any given time. So what is the prevailing zeitgeist amongst these particular populations? And is there a single one, or multiple, co-existing mindsets?

COMPANY EMPLOYEES

Let's start with the company employee, quite often and truly referred to as the most important company resource. It's certainly inarguable that the actions of an enterprise's individual employees are one of the most important factors on the scope and impact of a potential cybersecurity incident. Knowing this, CISOs for years have attempted to create a more "cyber savvy" workforce through a variety of tools: cybersecurity training, phishing tests, tabletop simulations (just to name a few).

IT IS OBVIOUS TO ALL THAT ALLOWING AN UNAUTHORIZED, BADGELESS INDIVIDUAL INTO A SECURE BUILDING IS A THREAT, BUT TRANSLATING THIS EQUIVALENT INTO THE DIGITAL WORLD IS EXTREMELY DIFFICULT FOR ANYONE WHO IS NOT A TECHNOLOGIST.

So why are we still in a place where most employees don't feel particularly empowered or educated? In fact, the emotion they express most often about cybersecurity is that it is "frustrating." Frustrating in all senses—either the employee has to contend with technology intended to make them safer, but that instead just gets in the way, or the employee is relied upon to make good cybersecurity decisions without having any particular cybersecurity expertise. This situation can also be frustrating for the CISO. If it's so straightforward for employees to understand that letting someone tailgate into a building is bad practice, then why isn't there the same intuitive understanding of the ills of password sharing?

Technology has moved so fast, and, driven by digital transformation, taken over so many of our ways of working, that we now have large numbers of company employees who understand how to use the technology but not actually how the technology works behind the scenes. It is obvious to all that allowing an unauthorized, badgeless individual into a secure building is a threat, but translating this equivalent into the digital world is extremely difficult for anyone who is not a technologist. As the pace of technology adoption, and the exponential curve of digital complexity increase, it is becoming more and more critical to consider the employee experience. Too often, technology is adding complexity and creating impediments to the employee function. This has an adverse effect not only on security but also on employee productivity overall.

OFFICERS AND DIRECTORS

Moving on to a smaller subset of the broader employee population, let's look at the C-suite and, by extension, the board of directors. The high-level strategic decisions made by company leaders have the potential to dramatically influence the cybersecurity posture of any given enterprise. This fact is well understood. For some years now it has been impossible to avoid discussing cybersecurity and its criticality in the boardroom and at the CEO level. What has been more elusive is how to translate that criticality into appropriate action and oversight.

Board directors and C-suite members are no strangers to risk discussions. It's not overly dramatic to say that risk discussions are literally the lifeblood of what the senior executives discuss and decide on every day. However, these risk discussions usually occur in a common, business-centric lexicon and relate to well-known topics such as the net present value (NPV) of a new project. Technology, and cybersecurity in particular, often bring their own jargon that can be difficult to put into analogous business terms. On the surface, the analogies between maintaining a fleet of company cars and maintaining a fleet of firewalls—software upgrades are like oil changes!—are obvious to practitioners but not obvious at all to business experts, who generally comprise the majority of board and C-level roles.

The outcome of this disconnect is the perception that cybersecurity is a new, strange animal when in reality it is business risk and opportunity in a different form. Without tech leaders and CISOs who can make that translation, the members of the C-suite and the board will continue to struggle to understand cybersecurity in relatable terms, impacting their ability to make optimum strategic decisions.

AVERAGE CITIZENS

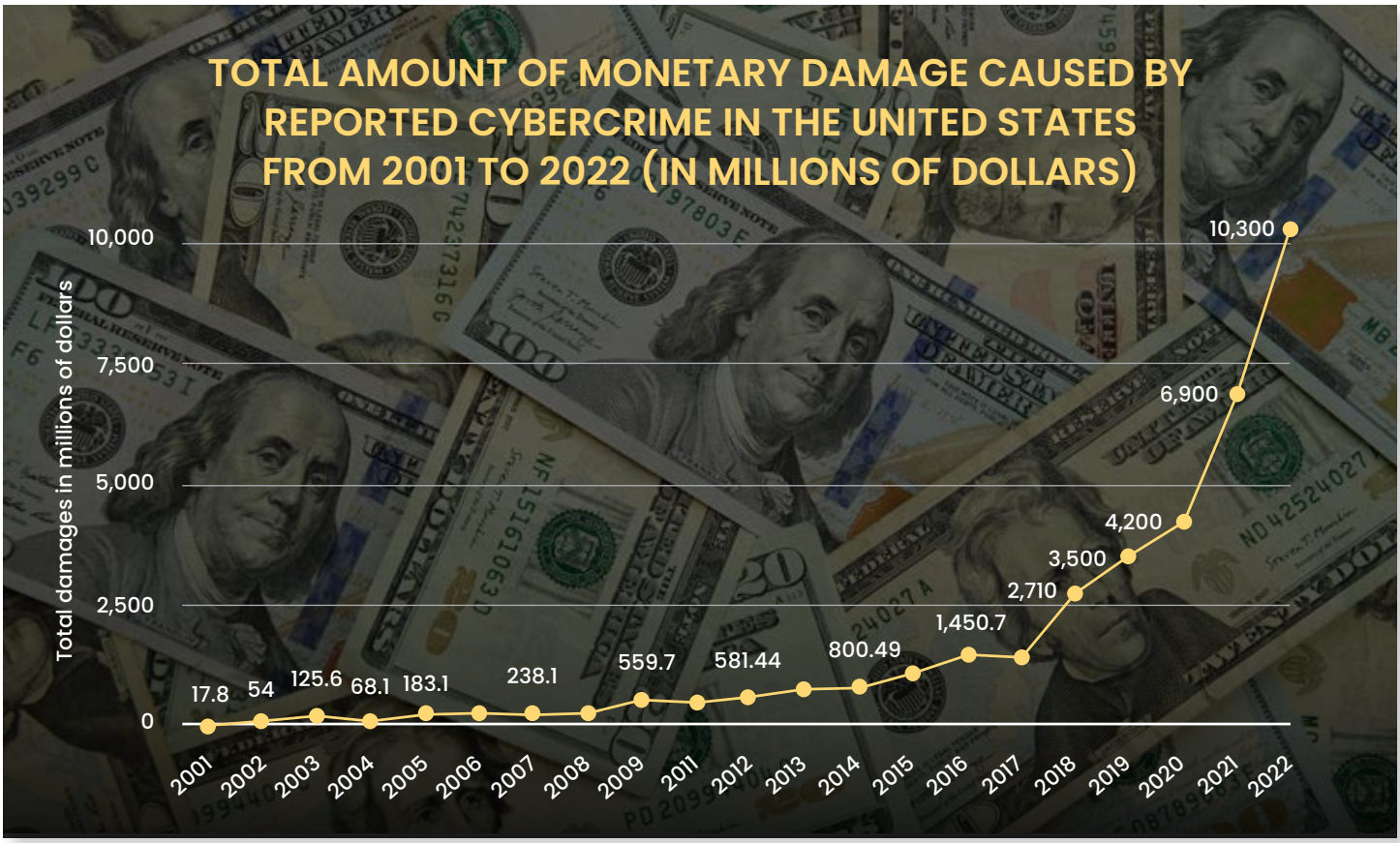
Now broadening the aperture, do we see similar states of mind in everyday citizens? Just as there's a disconnect between the 3D world and the digital world for the everyday worker, and between "business as usual" and cybersecurity for senior executives, we see people across society grapple with how to identify cyber threats and avoid joining the line of global victims. A similar analogy to the office tailgating example comes to mind. It is easy to understand how locking a door protects the house, or how putting a seat belt on protects the passenger in a car. It is extremely challenging for most people to intuitively understand what the equivalents are in the digital world to these basic protections.

The state of mind this has engendered is one of confusion, fear, and helplessness. When so much of life is digital, as it today, the effects of a cyberattack can be fundamentally destabilizing, if not life-threatening. The ability of average citizens to conceptually understand the digital tools that surround them, and then use that understanding to guide appropriate action, is not at the level needed for a "cyber-savvy" society. This can manifest, at one end of the spectrum, in extreme avoidance and mistrust of the digital ecosystem; and at the other end, in a complete reliance on the producers of technology to protect their user base.

THE BOTTOM LINE

In conclusion, there is no single "state of cybersecurity"—unless we want to posit that the state is one of fragmentation, with more opacity than clarity. Each population discussed here struggles to make parallels between their world as they know it, and how to avoid and/or mitigate cybersecurity threats.

While cybersecurity experts define and implement enterprise strategies, ultimately the bottom-line impact of cybersecurity on the lives of everyday people depends as much on those same people as it does on the experts. The ability to make good choices while living and working in the digital world will continue to require better conceptual models for understanding—and an increased focus on developing frictionless guardrails in the digital medium.



Source: Statista 2024

REDEFINING CYBERSECURITY

FROM DEFENSIVE MEASURES TO A STRATEGIC BUSINESS STRATEGY

DAVID NEUMAN, SENIOR ANALYST, TAG

In 2022, the monetary damage caused by cybercrime reported to the United States' Internet Crime Complaint Center (IC3) reached a historic peak of $10.3 billion, which represented a year-over-year increase of around 50%. This is despite 2023 global spending on cybersecurity and risk management reaching $181.1 billion. It's projected to rise to $215 billion in 2024. Given these numbers, why aren't we seeing a reduction in the cyber threat or in the material damage to businesses?

As industries grapple with the escalating digital complexity, sophistication of cyber threats, and the cost of defeating them, the traditional stance on cybersecurity—primarily focused on defensive technical operations and compliance—is proving to be ineffective. It is imperative to have a strategic pivot towards viewing cybersecurity through the prism of business enablement and risk management.

This change is driven by the need to safeguard assets and business operations and harness cybersecurity as a catalyst for competitive differentiation in the marketplace. It highlights the pressing need for cybersecurity to evolve in purpose from a defensive, technical posture to a proactive strategy that aligns with and propels business objectives. Moreover, it emphasizes the necessity for technologies and processes that are both adaptive and swift, mirroring the pace of business innovation. Through this lens, we gain clarity on why cybersecurity must transcend its traditional boundaries and be reimagined as a core component of business strategy, enabling organizations to navigate the digital age with confidence and strategic advantage.

IF YOUR SECURITY BUDGET IS BASED ON CONTINUING INCREASES THAT ARE TIED PURELY TO ADDITIONAL COSTS FOR MORE TECHNOLOGY PLATFORMS VERSUS BUSINESS OUTCOMES, THEN YOU ARE LIKELY NOT PROVIDING A COMPETITIVE ADVANTAGE.

THE LEGACY MINDSET: A BUSINESS STRATEGY DISASTER

For too long, the prevailing approach to cybersecurity has been reactive. Too often products and services are designed with functionality as the primary focus, and security is bolted on as an afterthought. This leads to weaknesses attackers can exploit, resulting in costly redesigns, reputational damage, and potential fines for noncompliance.

"Security by design" means baking security into the development process from the outset. The alternative can lead to disaster. For example, a software company releases a new product with exciting features but fails to incorporate security. The product is riddled with vulnerabilities, leading to a major data breach that erodes customer trust and forces costly remedial efforts. We saw this recently in the attack against Microsoft Exchange Online. As reported by the DHS Cyber Safety Review Board, the breach was attributed to Chinese espionage and advanced threat actors who accessed U.S. government agencies involved in sensitive diplomatic issues with China. This suggests the problem affects enterprises and companies of all sizes. We can all do better.

Many organizations rely on static security architectures that are ill-equipped to handle the dynamic nature of today's business environments. An enterprise that relies on a rigid security architecture, if they have one at all, will struggle to adapt to the rapid adoption of cloud services and artificial intelligence, among other digital imperatives. This creates security blind spots, exposing the organization to new attack vectors and slowing growth.

If your security program or IT and product platforms have not adopted this approach under the guidance of experienced experts, then you are likely accepting significant business risk. On the other hand, if your company's architectures are flexible and can evolve alongside changes in technology, business processes, and the threat landscape, cyber resiliency can be a competitive advantage.

CYBER LEADERS AS BUSINESS LEADERS

Cybersecurity leaders often lack the business acumen needed to effectively communicate risks and justify security investments to business partners and corporate leaders. This disconnect can lead to underinvestment in cybersecurity and a failure to align security initiatives with broader business objectives. It's crucial to bridge this gap between technical experts and business leaders to have a deep understanding of business strategy.

TAG Infosphere tracks over 4,700 cybersecurity vendors in a taxonomy of 20 categories. In a recent conversation with a chief information security officer (CISO) of a large enterprise, I asked, "How many of these taxonomy categories do you have a a technology in? His response was, "All of them. In fact, I have as many as three technologies for some of them." We agreed that more tools do not mean better security and don't necessarily equal business enablement. Many CISOs are trapped in sustaining these large security ecosystems, making it difficult for them to adapt to business demands and contribute to the growth the company is trying to achieve.

1. APPLICATION SECURITY	11. IDENTITY AND ACCESS MANAGEMENT (IAM)
2. ATTACK SURFACE MANAGEMENT	12. SECURITY OPERATIONS AND RESPONSE
3. AUTHENTICATION	13. MANAGED SECURITY SERVICES
4. CLOUD SECURITY	14. MOBILE SECURITY
5. DATA SECURITY	15. NETWORK SECURITY
6. EMAIL SECURITY	16. OPERATIONAL TECHNOLOGY SECURITY
7. ENCRYPTION AND PKI	17. SECURITY PROFESSIONAL SERVICES
8. ENDPOINT SECURITY	18. SOFTWARE LIFECYCLE SECURITY
9. ENTERPRISE IT INFRASTRUCTURE	19. THREAT AND VULNERABILITY MANAGEMENT
10. GOVERNANCE, RISK, AND COMPLIANCE (GRC)	20. WEB SECURITY

TAG Cyber Taxonomy

If your security budget is based on continuing increases that are tied purely to additional costs for more technology platforms versus business outcomes, then you are likely not providing a competitive advantage. Nor are you addressing the business risks for your organization. As indicated above, many security programs have duplicative technologies performing highly similar functions. This means higher complexity, costs, and a demand for highly skilled people. The result may be the equivalent of a two-mile freight train going five miles an hour, unable to move or change at the speed of the business.

We are seeing rightsizing in the cybersecurity technology market, which indicates that many security organizations, especially those in large enterprises, are rationalizing their existing portfolios instead of buying more technology solutions. That is a step in the right direction. Still, the rationale must include more than the technological capability and extend to ensuring that the solutions map a path to business outcomes, and that talent development and growth are part of it.

THE PATH FORWARD: CYBER RESILIENCY AND TRUST AS STRATEGIC ENABLERS

If your organization is considering a real pivot, there are some things you should consider. No two organizations are identical, and there are no easy buttons, so it's impractical to suggest a common playbook. But some focus areas are a good starting point.

1. ESTABLISH SHORT AND LONG-TERM PLANNING.

Many organizations claim to do strategy when what they are doing is planning—for their own teams and business units. In some cases, this is understandable. It may be because the organization lacks a comprehensive strategy. But in most cases the security organization is unaware of the business objectives and how they fit in. This isn't a company problem; it's a security problem. If you are doing any strategy or planning and have no direct insight or influence in what the business is doing, you are likely creating disruptions instead of enablement.

Your strategy should always begin with the business ambitions and desired outcomes. A series of questions arises from those insights. Are you positioned, with existing capabilities and services, to enable the outcomes the business seeks—near- and long-term? If you are not, can you adjust or rationalize your portfolio? Last, do you have the right skills and leadership to work with other business stakeholders? If the answer to any of these questions is no, you should consider fundamental changes to your strategy.

If your answer to these questions is yes, start influencing the messaging among external stakeholders that cyber resiliency and trust are differentiators. It may sound like a play on words, but you may be able to stop focusing on security and instead change your company's value generation story as part of product and service delivery.

2. SET RISK EXPECTATIONS AND SPEAK CLEARLY.

The security community has far too many cliches and tag lines the business doesn't understand and can't relate to. "Defense in depth is key to our cybersecurity strategy." "Zero trust is the future of security." "We must stay vigilant against advanced persistent threats." These make it hard for others you need for support to understand what you do and why it's important. Additionally, security teams all too often talk about what they do and not the business or the market they serve. Instead of spending time explaining advanced persistent cyber threats, try putting your concerns in terms of potential business disruption and what that could mean to your customers or business partners. Spend time spreading awareness of the risks in your market. Let your customers know what you do and why, and how your approach differentiates you from your competitors.

What you don't do is sometimes just as important as what you do. The security team cannot accept business risk on its own because it doesn't own much of the business it is charged to protect. In addition, not every cyber risk requires a cyber solution. This means emphasizing that not all issues in the realm of cybersecurity can be effectively addressed solely through technological or security means. For example, cybersecurity risks can also arise from weaknesses in the supply chain, where third-party vendors or partners may inadvertently introduce risks into an organization's systems and networks.

While implementing cybersecurity measures within one's organization is important, it may not be sufficient to address supply chain risks that lead to operations disruption or that compromise product integrity. You're going to get attacked—embrace it and prepare for it. This is what it means to be resilient. There are risk tolerance guardrails the security team must help business stakeholders understand so that they can participate in remediation (and value generation), and, more importantly, so that they won't make incorrect assumptions about their risk exposure.

3. BUILD AN ADAPTIVE AND HIGH-PERFORMING TEAM.

A 2023 report from the International Information Systems Security Certification Consortium (ISC2) highlights a shortage of almost four million cybersecurity professionals globally. Frankly, I don't buy it. I'm not suggesting that ISC2 has done something wrong. Still, there is too much ambiguity in our jobs and the positions we need to fill. And our existing workforce lacks professional development. We also are

addressing only our needs today and yesterday instead of focusing more attention on the organization we'll need to be tomorrow. To seize the opportunities of tomorrow, we must develop a workforce of innovative thinkers and creative doers, not just technical experts. This entails personal and professional skills, including the ability to communicate, understand how an organization is organized and operates, and build relationships. The skills are essential in building a resilient organization.

As an adjunct university professor who teaches cyber operations and threat hunting, I ask students about their career ambitions. They almost unilaterally say, "I want to work in cyber." When I ask for more specifics, they seem lost. Why is that? I believe we have produced a generation of security tool administrators when we need critical and analytical thinkers and problem solvers. The security industry needs to drive the demand for more of these thinkers and fewer holders of professional certifications, which have become an industry themselves.

Too often security team member development is relegated to technical competency training. I'm not suggesting this is wrong; it's just incomplete. If technical skills are all a person brings to the table by the time they are promoted into leadership positions, they will be disadvantaged, as will the organizations they belong to. We must build well-rounded teams to solve business risk problems and take advantage of opportunities beyond security and technology. If deliberate training, development, and career progression plans are discretionary budget items, companies will not recruit or retain the top talent needed to compete and succeed. People are vital to the effective execution of strategy.

4. WORK TO ACHIEVE OPERATIONAL EXCELLENCE.

Organizations must transcend procedural efficiency and evolve into dynamic learning entities, constantly honing their defenses against ever-shifting threats. Embracing a learning organization mindset, they foster curiosity, innovation, and a relentless pursuit of improvement throughout their organization.

This approach entails more than just investing in technical prowess; it's about cultivating a collective intelligence that thrives on feedback, reflection, and shared knowledge. By promoting ongoing training, encouraging experimentation, and institutionalizing robust incident response processes, organizations equip themselves to navigate the complexities of modern cybersecurity with agility and resilience. Moreover, they recognize that cyber resiliency is not a static discipline but a fluid landscape where adaptability and innovation are paramount.

Ultimately, by prioritizing a culture of continuous improvement, organizations elevate their capabilities from reactive measures to proactive planning. They leverage each encounter with cyber threats as an opportunity for growth, distilling insights from successes and failures alike. Through this commitment to learning and evolution, organizations fortify their posture against cyber exploitation, safeguarding their digital assets and resilience in an increasingly hostile digital landscape.

FINAL THOUGHTS

The consequences of outdated approaches are significant. Companies find themselves locked in a never-ending arms race against cybercriminals and nation-state threat actors, constantly pouring resources into upgrading defensive technology. This leads to bloated cybersecurity budgets that drain resources from more value-adding initiatives. In addition, the reactive nature of legacy security models often results in a material impact on companies and their customers. According to IBM's report on the Cost of a Data Breach 2023, the average is $4.45 million. The reputational damage can be even more devastating, eroding customer trust and hindering long-term growth.

SWIMLANE

Swimlane delivers automation for the entire security organization. Swimlane Turbine is the AI-enabled, **low-code security automation** platform that unifies security teams, tools, and telemetry in-and-beyond the SOC into a single system of record to reduce process and data fatigue while quantifying business value and ensuring overall security effectiveness.

TAG
DISTINGUISHED VENDOR

REPRINTED FROM THE TAG SECURITY ANNUAL