

2024

TAG

Security Annual

SPECIAL REPRINT EDITION

REVOLUTIONIZING THREAT DETECTION WITH DECEPTION

AN INTERVIEW WITH RAM VARADARAJAN,
CO-FOUNDER AND CEO, ACALVIO TECHNOLOGIES

WHY NATION-STATES ARE VULNERABLE TO QUANTUM THREATS RIGHT NOW

THE STATES OF CYBERSECURITY

REDEFINING CYBERSECURITY:
FROM DEFENSIVE MEASURES TO A STRATEGIC BUSINESS STRATEGY

TAG
DISTINGUISHED VENDOR

ACALVIO
AI-POWERED DECEPTION

The need to reduce cyber risk has never been greater, and Acalvio has



demonstrated excellence in this regard. The TAG analysts have selected Acalvio Technologies as a 2024 Distinguished Vendor, and such an award is based on merit. Enterprise teams using Acalvio’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

REVOLUTIONIZING THREAT DETECTION WITH DECEPTION

An interview with Ram Varadarajan,
Co-founder and CEO, Acalvio Technologies

3

WHY NATION-STATES ARE VULNERABLE TO QUANTUM THREATS RIGHT NOW

Dr. Edward Amoroso, Senior Analyst, TAG

7

THE STATES OF CYBERSECURITY

Joanna Burkey, Senior Analyst, TAG

10

**REDEFINING CYBERSECURITY:
FROM DEFENSIVE MEASURES TO A STRATEGIC BUSINESS STRATEGY**

David Neuman, Senior Analyst, TAG

13

REPRINTED FROM THE TAG SECURITY ANNUAL

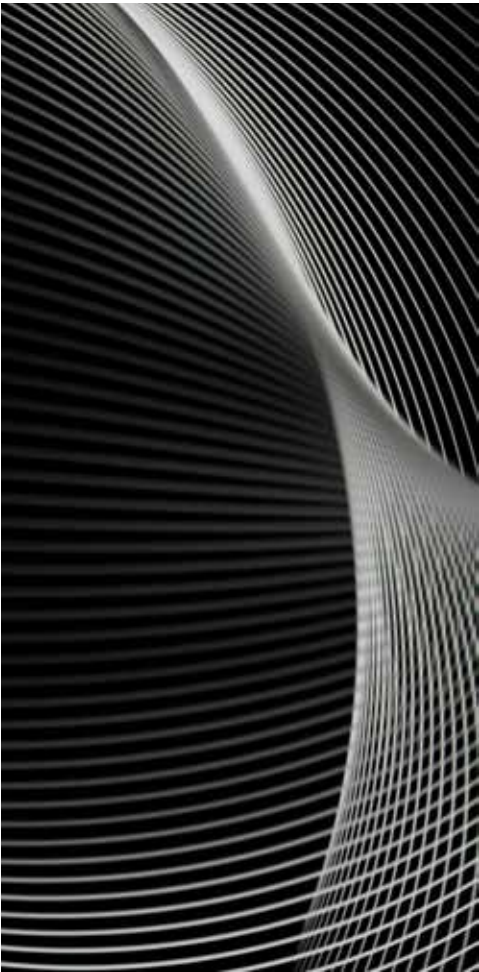
©TAG INFOSPHERE, INC. 2024



AN INTERVIEW WITH RAM VARADARAJAN,
CO-FOUNDER AND CEO,
ACALVIO TECHNOLOGIES

REVOLUTIONIZING THREAT DETECTION WITH DECEPTION

As cybersecurity threats grow increasingly sophisticated, Acalvio's ShadowPlex solution redefines how organizations detect and mitigate advanced attacks. By combining AI and cyber deception, ShadowPlex provides a proactive defense strategy that addresses gaps in traditional tools. In a recent chat with Acalvio, we explored how this platform improves SOC efficiency, enhances threat-hunting capabilities, and integrates seamlessly into enterprise workflows.



TAG: How does the AI-enhanced approach of ShadowPlex provide a unique advantage over traditional security solutions that focus on signature-based detection?

ACALVIO: We leverage advanced cyber deception technology combined with AI for proactive threat detection. Unlike traditional signature-based solutions that only recognize known threats, our approach identifies modern, evasive tactics like polymorphic malware and identity compromises. Acalvio's technology sets traps tailored to the attacker's goals, ensuring that any interaction triggers an immediate alert for defenders.


Acalvio's solutions effectively detect known and unknown threats, including zero-days. Defense teams need a comprehensive deception strategy to maximize threat detection across diverse vectors. Acalvio employs AI to optimize the count, type, and placement of deceptions in the environment. For instance, Acalvio's AI automates the creation of realistic attribute values for the over 100 attributes needed for each user account in Active Directory..

Acalvio AI enhances deception by strategically introducing misconfigurations that entice attackers to target deceptive assets over real ones, such as creating a deceptive Kerberoastable account to identity threats. Their deception techniques cover various MITRE tactics, including Credential Access, Lateral Movement, Defense Evasion, Privilege Escalation, and Exfiltration.

TAG: Can you elaborate on how ShadowPlex distinguishes between legitimate user actions and potential adversarial activity, especially in environments where traditional security tools may fail?

ACALVIO: ShadowPlex has a unique approach based on cyber deception that sets traps for the attacker based on the attacker's goals and independent of the attacker's TTP. For example, in an Active Directory environment, ShadowPlex deploys deceptive user accounts and service accounts as honeypots. The deceptions are not used in existing IT or business workflows, eliminating the challenge of distinguishing between legitimate user actions and adversarial activity. Any usage of the honeypots is indicative of attacker activity, providing defense teams with a high-fidelity alert. This is a highly effective approach to detect threats where traditional security tools may fail.

Unlike traditional signature-based solutions that only recognize known threats, our approach identifies modern, evasive tactics like polymorphic malware and identity compromises.



TAG: *How does Acalvio's threat-hunting workbench leverage deception technology to offer more precise and proactive threat identification?*

ACALVIO: Traditional threat-hunting methods typically focus on Indicator of Compromise (IoC) sweeps and log searches. While useful, these can be time consuming and resource intensive. Acalvio introduces a novel approach through a precision workbench, which utilizes specific deceptions for threat hunting. These deceptions offer controlled opportunities to detect threats, identify latent malware, and validate hunting hypotheses. For instance, threats may lie dormant, waiting to exploit vulnerabilities in legacy systems using SMBv1, like EternalBlue. Threat-hunting teams can use the ShadowPlex workbench to deploy a decoy with SMBv1, allowing them to lure the latent threat and confirm their hypothesis as part of a proactive, precise hunting strategy.

In addition, ShadowPlex threat hunting workbench provides precision analytics capabilities, such as Memory forensic analysis to identify stealthy, in-memory threats that have evasive techniques, such as Process Hollowing that are challenging to detect, PowerShell script and log analysis to find threats that leverage obfuscated PowerShell scripts to perform malicious activity, and adversary traversal analytics that leverages AI to enable hunting teams to find the set of additional endpoints likely to have been on the pathway of the adversary and need investigation as part of the hunting actions.

TAG: *ShadowPlex integrates with EDR, XDR, SIEM, and SOAR tools. How does this interoperability benefit enterprise SOC teams, and what specific efficiencies does it bring to incident response workflows*

ACALVIO: ShadowPlex integrates with EDR and XDR platforms to automate endpoint discovery for deploying realistic deceptions, facilitate agentless honeypot updates, and initiate automated threat response workflows. Its integration with SIEM enhances SOC visibility by consolidating alerts into a single interface, eliminating the need to access the ShadowPlex console. Alerts are auto-triaged and aligned with the MITRE ATT&CK framework, streamlining incident response by removing manual deduplication and providing a standardized taxonomy for SOC teams. .

ShadowPlex integrates bi-directionally with SOAR platforms, directly sending high-fidelity to the SOAR. This functionality enhances incident response workflows by making alerts immediately actionable, simplifying SOAR response playbooks, and enabling rapid isolation of threats. Additionally, ShadowPlex allows for the dynamic deployment of extra deceptions to slow down attackers and collect targeted forensics from compromised endpoints to investigate attacker persistence.

TAG: How do ShadowPlex's auto-triaged alerts contribute to reducing detection windows, and how does this impact overall SOC efficiency and threat response?

ACALVIO: Traditional alerting mechanisms capture individual alerts and send all the events to the SIEM. This requires SOC teams to perform manual triaging actions involving event deduplication, correlation with other event sources, enrichment, and summarization. These actions require human expertise and involvement, requiring time for the investigation phase and increasing the detection window. ShadowPlex performs automated triaging of the deception events, generating actionable alerts for SOC that can be immediately acted on without requiring additional triaging or post-processing. For example, consider a fast-propagating threat that attempts to propagate over SMB protocol across the environment.

ShadowPlex observes the SMB attempts across multiple decoys, performs automated triaging of the individual decoy events, and surfaces an actionable alert that provides evidence of the compromised endpoint. The auto-triaged alerts are high-fidelity and do not have false positives, enabling automated response actions to be performed to stop the threat before adversary breakout. This greatly reduces the detection window, an imperative step for cyber defense, as the threats leverage automated tooling for rapid propagation.



WHY NATION-STATES ARE VULNERABLE TO QUANTUM THREATS RIGHT NOW



DR. EDWARD AMOROSO

We know organizations that have relied on encryption to protect sensitive information will soon be grappling with the implications of a post-quantum era, where today's encryption protocols could be rendered obsolete. The concern surrounding store-now-decrypt-later methods is particularly pressing for organizations dealing with adversaries such as nation-states.

Our concern at TAG is that the most capable nation-state actors are often decades ahead in cryptographic research and espionage. As a result, we must assume that they are already gathering encrypted data with the intention of decrypting it when quantum computers become sufficiently powerful. But perhaps we should fear that sufficiently strong quantum computers might already exist in the basements of these powerful organizations.

Most businesspeople and technologists have been told by organizations such as the National Institute of Standards and Technology (NIST) that the timeline to Y2Q (year to quantum), when quantum computers will be able to crack widely used encryption, is still many years away. But in this article, we try to make the reasonable case that Y2Q could be much closer than most organizations realize, especially if their adversaries are nation-states, like the ones that are home to the NSA and GCHQ.

THE STORE-NOW-DECRYPT-LATER THREAT

This concept is a strategy that hinges on the expectation that while today's encryption remains robust, it can be broken in the future when quantum

computers reach a certain level of sophistication. Nation-states and advanced threat actors are believed to be intercepting and storing vast quantities of encrypted data, knowing that it is only a matter of time before they can break it.

Classical encryption algorithms, such as RSA and ECC (Elliptic Curve Cryptography), rely on the computational difficulty of problems like integer factorization and discrete logarithms. These problems are considered intractable for classical computers, but quantum computers can solve them exponentially faster using Shor's algorithm. This means that once sufficiently powerful quantum computers are operational, these encryption standards will be broken.

The presumed danger for organizations is that once their encrypted data is compromised, it may already be too late. Sensitive data, including state secrets, intellectual property, financial transactions, and personal information, can be accessed retroactively, leading to breaches. It's not just about future communications being compromised—it's about everything that has been encrypted up until now being cracked once quantum decryption becomes viable.

But this is the rub: Everyone assumes that nation-state actors are no farther along in their quantum research than every other research and development team in the world (e.g., IBM). Experience dictates that this could be wrong. Remember, for example, that James Ellis invented public key cryptography at GCHQ half a decade before Diffie and Hellman.

NATION-STATES ARE AHEAD: THE NSA AND GCHQ

In fact, our view is that by any reasonable historical analysis, intelligence agencies like the NSA and GCHQ have been significantly ahead of the public cryptographic community. From early advances in cryptographic analysis during World War II to their leadership in digital encryption, these agencies have often been at the forefront of both creating and breaking encryption technologies—and they attract and employ the best talent.

The NSA's involvement in cryptography is particularly significant. It is widely believed that the NSA has had access to cryptanalytic techniques and computational resources far beyond what is known publicly. For example, the declassification of Cold War-era ciphers showed that the U.S. intelligence community had broken encryption methods long before the public cryptographic community believed them to be insecure.

While no government has openly declared having a fully operational quantum computer, it is not unreasonable to suspect that research divisions within organizations like the NSA or GCHQ have quantum computing capabilities in development. Given the high stakes of cyber warfare and espionage, these agencies likely have substantial quantum cryptanalysis programs aimed at foreign adversaries and even private organizations.

From the perspective of TAG, we fully admit to our national and geographic bias toward viewing the NSA and GCHQ as benevolent organizations. (And yes, we know that many of our readers will disagree.) That said, we would point out that many nation-state actors should not be viewed as so benevolent, and this is where we are most concerned. Readers can fill in their country of choice, but it seems reasonable that adversary nations are working in this area.

**SENSITIVE DATA,
INCLUDING STATE
SECRETS, INTELLECTUAL
PROPERTY, FINANCIAL
TRANSACTIONS, AND
PERSONAL INFORMATION,
CAN BE ACCESSED
RETROACTIVELY, LEADING
TO BREACHES.**



NIST'S QUANTUM THREAT TIMELINE MAY BE TOO CONSERVATIVE

NIST has been at the forefront of preparing the cryptographic community for the quantum threat. In 2016, NIST began a process to evaluate and standardize post-quantum cryptography (PQC) algorithms that are resistant to quantum attacks. NIST's official timeline for when quantum computers will be able to break classical encryption has been estimated to be between 10 and 20 years from now.

This timeline is based on several assumptions about the pace of quantum computing development, the technical hurdles that must be overcome, and the scale of quantum computers needed to break classical encryption. However, several experts believe this estimate is outdated and fails to account for the accelerated pace of quantum research or the secrecy surrounding nation-state programs.

We believe that for organizations dealing with sensitive information, the quantum threat is already here. These organizations cannot afford to assume that Y2Q is decades away, particularly given the possibility that adversarial nations are further along in their quantum capabilities than public research suggests. If such nations already have quantum computers capable of breaking encryption protocols, then Y2Q is effectively now.

RAPID ADVANCES IN QUANTUM COMPUTING

As further evidence, consider that the field of quantum computing is advancing rapidly. In recent years, companies like IBM, Google, and Honeywell have made significant strides in developing more powerful and stable quantum processors. Google famously announced in 2019 that it had achieved "quantum supremacy," demonstrating that a quantum computer could solve a problem faster than the world's most powerful classical supercomputer.

Quantum hardware is also steadily improving, with qubit counts rising and error rates decreasing. Researchers are also developing new techniques for error correction, a major hurdle in quantum computing, which will allow quantum computers to scale more effectively. With these improvements, the gap between theoretical quantum cryptanalysis and practical deployment is closing faster than anticipated.

Several governments, including China's, have also invested heavily in quantum research. China's quantum efforts are of concern to the West, as the country has demonstrated leadership in quantum communication and quantum cryptography. Chinese research in quantum key distribution (QKD) and other aspects of quantum security suggests that the country is pursuing quantum dominance, which would have significant geopolitical implications.

PREPARING FOR THE QUANTUM THREAT

For organizations concerned with the quantum threat, the time to act is now. Waiting for public announcements of quantum breakthroughs could leave them vulnerable. Instead, organizations should begin transitioning to quantum-resistant cryptographic protocols as part of a broader post-quantum security strategy. NIST's ongoing work to standardize PQC algorithms provides a roadmap for this transition, but organizations must start preparing immediately.

Additionally, organizations should assess their long-term data protection needs. If encrypted data today is expected to retain its sensitivity for decades, then the risk of it being decrypted by future quantum computers is significant. By adopting quantum-resistant encryption methods today, organizations can mitigate the risk posed by store-now-decrypt-later strategies employed by adversaries.



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).

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.

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.

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.

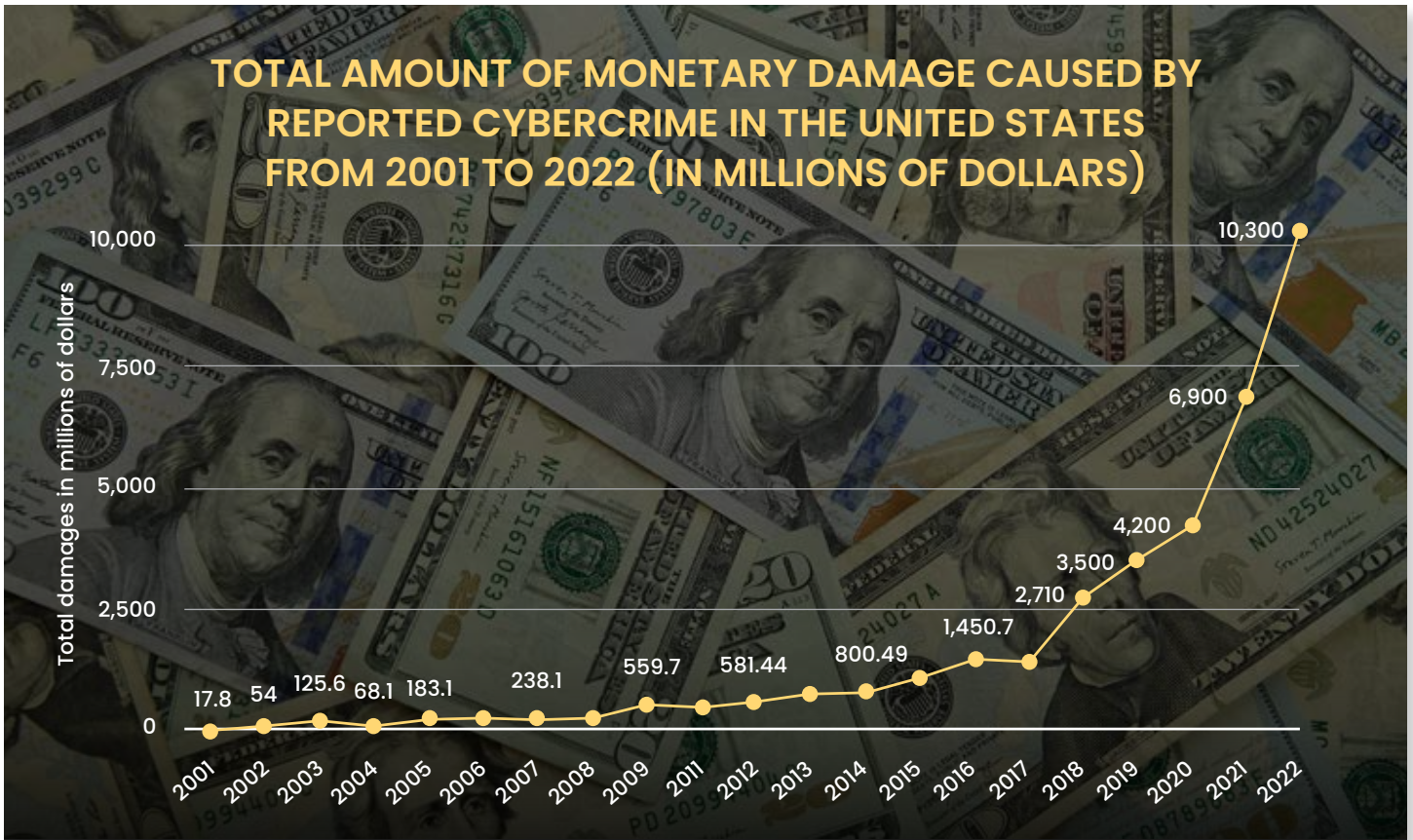


The state of mind this has engendered is one of confusion, fear, and helplessness. When so much of life is digital, as it today, the effects of a cyberattack can be fundamentally destabilizing, if not life-threatening. The ability of average citizens to conceptually understand the digital tools that 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.

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.

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.

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 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.



AI-POWERED DECEPTION

Acalvio is the leader in autonomous cyber deception technologies, offering enterprises early detection of sophisticated cyber threats, including APTs, identity exploits, insider threats, and ransomware. Its AI-powered ShadowPlex Platform, backed by 25 patents, shifts power from attackers to defenders across IT, OT, and Cloud and enhances Zero Trust security models.



REPRINTED FROM THE TAG SECURITY ANNUAL

©TAG INFOSPHERE, INC. 2024