As Budgets Get Tighter, Cybersecurity Must Get Smarter

BCG's Annual Cybersecurity Survey 2023

APRIL 24, 2023

By Clark O'Niell, Varun Khurana, Colin Troha, Braden Holstege, Nadya Bartol, Alex Asen, Geoffrey Cheung, Matthew Fallon, and Bernhard Gapp

READING TIME: 12 MIN

The role of the Chief Information Security Officer (CISO) in 2023 involves dealing with two competing pressures. The world of cyber hazards continues to expand, driven by proliferating traditional threats and emerging attack vectors such as AI-enabled social engineering. At the same time, deteriorating economic conditions require cybersecurity leaders to make do with the smallest budget increases in recent memory.

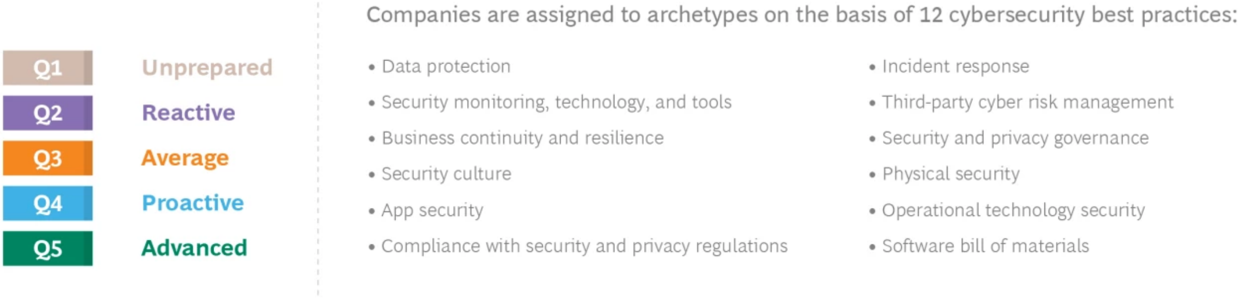
As companies seek optimal ways to manage these contradictory forces, the landscape of cybersecurity will change in important ways:

- Relatively mature categories of cybersecurity solutions will face pressure leading toward vendor consolidation. As a result, they will tend to coalesce into five natural control points: operating systems, cloud security, endpoint security, networking and zero-trust security, and corporate identity.
- At the same time, CISOs will experiment with new cybersecurity solutions. Vendors will continue to proliferate in emerging categories such as application programming interface (API) security and cloud security.
- CISOs will be pressed to explore increased training, process improvements, and shifts in corporate culture to improve their security postures without expanding their budgets.
- ROI—in comparative terms and in absolute terms—will become a key component of vendors' sales proposition.
- Investors must ride the wave of consolidation, identifying solutions that avoid competitive pressure and investing either in emerging categories or in niche players.

Economic Pressures

These dynamics take center stage in BCG's most recent annual survey, of 600 cybersecurity leaders from companies around the world, conducted in March 2023. In collaboration with GLG, an insight network that provides access to expert perspectives, BCG asked 600 CISOs, cybersecurity professionals, and adjacent stakeholders about their priorities, expectations, current and future budgets, and technological resources, as well as about the pressures facing them. About two-thirds of the respondents work in enterprises with more than 2,000 full-time equivalent employees, and the rest in smaller businesses. Geographically, 70% of the respondents are based in the Americas, with others located in Europe, the Middle East, and the Asia-Pacific region.

Exhibit 1 - Five Archetypes of Cyber Maturity



Q1	Unprepared
Q2	Reactive
Q3	Average
Q4	Proactive
Q5	Advanced

Companies are assigned to archetypes on the basis of 12 cybersecurity best practices:

- Data protection
- Security monitoring, technology, and tools
- Business continuity and resilience
- Security culture
- App security
- Compliance with security and privacy regulations
- Incident response
- Third-party cyber risk management
- Security and privacy governance
- Physical security
- Operational technology security
- Software bill of materials

Sources: BCG and GLG CISO Cybermaturity Survey and Scorecard; BCG analysis.

Note: All survey respondents were categorized via self-assessment, calibrated through an analysis of answer distribution (to adjust for bias) and actual product adoption (as a cross-check). Overall scores were normalized to exclude nonapplicable practices.

On the basis of respondents' assessments of their own companies' practices, we divided companies into five quintiles, each representing a distinct archetype of cybersecurity maturity (or "cyber maturity"): unprepared, reactive, average, proactive, and advanced. (See Exhibit 1.)

Overall, the survey responses suggest that CISOs feel pressure to do more with less this year—a challenge that many haven't faced previously. In economically stable times, CISOs would expect their budgets to rise about 8% per year. But on average, in a recessionary environment, CISOs expect to see a rise of only 4% from the previous fiscal year. Meanwhile, they expect vendor prices to increase by about 3% to 5% year-on-year. In other words, the effective value of their procurement budget has either remained level or declined slightly. Although vendor prices tend to level off during a recession, too, the result would be an effective contraction of about 1% across most companies.

Learning from Advanced Organizations

In this environment, only companies that fall into the most advanced of our five cyber maturity archetypes have the luxury of time to consider emerging threats, and the resources to prepare for them. They spend approximately $1,300 to $1,400 per FTE, whereas most companies—those in the unprepared, reactive, average, and proactive archetypes—spend up to $500 to $600 per FTE.

All survey respondents were attentive to threats they already knew, such as ransomware. (See Exhibit 2.) More than two-thirds of respondents also expressed concerns about cloud cybersecurity, changing regulations, and third-party cybersecurity risks. Concerns about attracting talent, supporting remote work, and controlling costs ranked close behind.

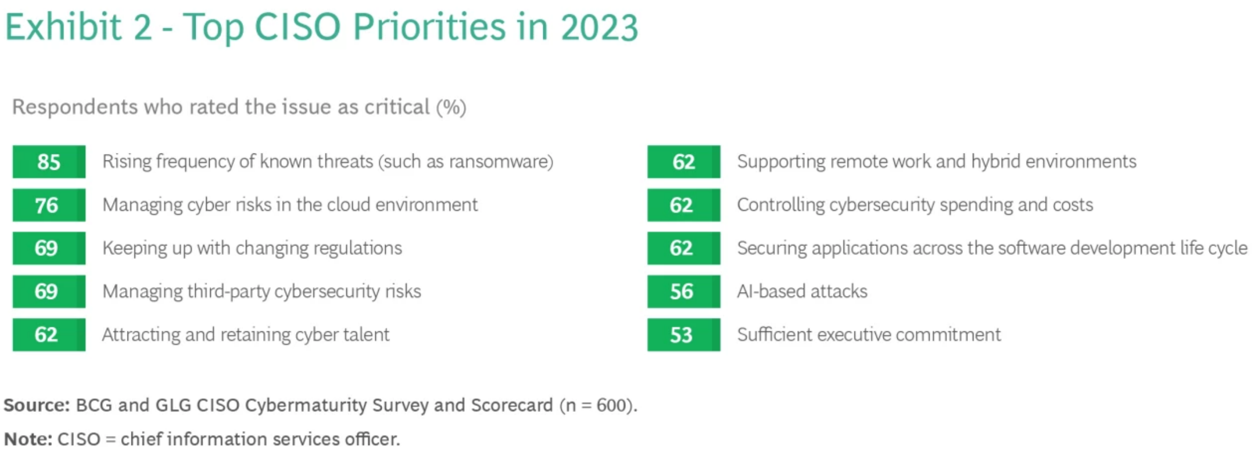


Exhibit 2 - Top CISO Priorities in 2023

Respondents who rated the issue as critical (%)

85	Rising frequency of known threats (such as ransomware)
76	Managing cyber risks in the cloud environment
69	Keeping up with changing regulations
69	Managing third-party cybersecurity risks
62	Attracting and retaining cyber talent
62	Supporting remote work and hybrid environments
62	Controlling cybersecurity spending and costs
62	Securing applications across the software development life cycle
56	AI-based attacks
53	Sufficient executive commitment

Source: BCG and GLG CISO Cybermaturity Survey and Scorecard (n = 600).

Note: CISO = chief information services officer.

Respondents from advanced companies tended to share these concerns, but they also paid attention to future threats. Among this smaller group, 74% said that the threat of AI-based attacks was a critical concern, and 73% said the same about AI-enabled social engineering. These responses reflected other aspects of their culture: stronger employee awareness of security issues, and greater executive support for cybersecurity investment. Because these companies have basic cybersecurity capabilities in place, their CISOs have the backing and capacity to think innovatively about meeting the coming wave of threats.

Among the practices that differentiate these more farsighted companies is an emphasis on return on investment (ROI). About 56% of advanced firms' CISOs said that they consistently measure ROI for their cybersecurity spending. By contrast, only 39% of the overall survey respondents reported consistently measuring ROI for cybersecurity spending. For companies in the unprepared archetype—the bottom quintile of cyber maturity—the figure was 22%.

Advanced companies gain their ROI by deploying skilled people, well-designed processes and up-to-date technologies. In the advanced group, 48% deploy network detection and response (NDR), a cybersecurity strategy that involves consistently tracking communications patterns to detect, investigate, and respond to threats that might otherwise remain hidden. Use of application security testing (AST) to identify vulnerabilities in source code is championed by 42% of the same group, and cloud workload protection (CWP), which entails monitoring cloud services for potential threats, by 38%. These higher-than-average adoption rates among advanced companies reflect the companies' nature as early adopters and the very recent emergence of the technologies. At the same time, these percentages indicate that there is much room for improvement and more need for best practices—even among advanced companies.

The Consolidation Trend

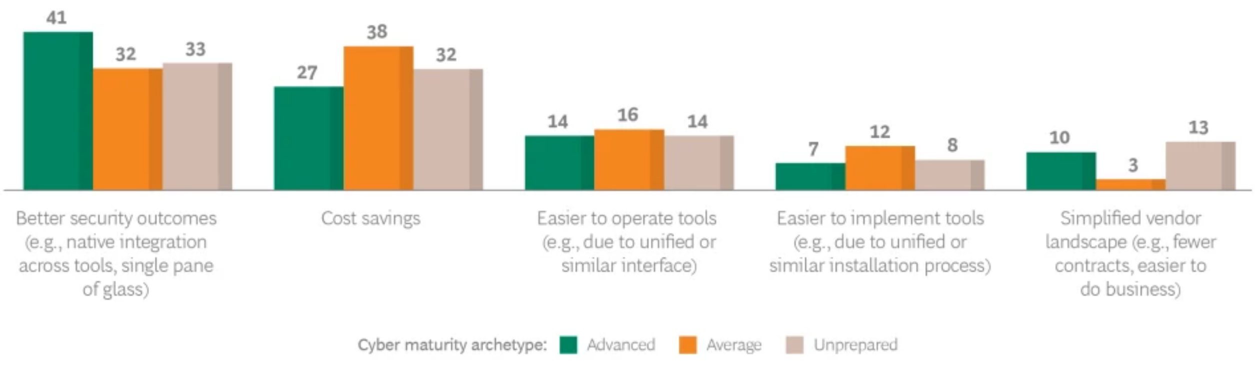
This year, many cybersecurity leaders reported that they are looking for larger, consolidated vendors that can provide multiple services in a single offering. CISOs say that mature cybersecurity technologies —traditional endpoint protection platforms, firewalls, governance risk and compliance services, network access control, secure email gateways, and unified endpoint management— offer the highest level of bundling. In these categories, the percentage of survey respondents looking to consolidate is larger than the percentage looking to expand procurement.

A few other solutions also involve mature technologies, but for a variety of reasons they are less likely candidates for consolidation or expansion. These offerings include risk management solutions from IT vendors, secure web gateways, user authentication and access management solutions, and endpoint detection and response systems.

In general, advanced companies think differently about sourcing security capabilities than the other companies do. For example, many companies are now consolidating their cybersecurity vendors. When asked about their reasoning, most CISOs cited cost savings as the primary motive. CISOs from advanced companies, however, said that they were looking for improved security outcomes. Evidently, they view having fewer vendors but more robust integrated relationships with those vendors as a way to achieve both goals. (See Exhibit 3.)

Exhibit 3 - Each Cybersecurity Archetype Has Its Own Motives for Consolidating Vendors

Q: For tools where you prefer a bundled solution, what is your primary reason? (%)



Source: BCG and GLG CISO Cybermaturity Survey and Scorecard (n = 600).

Five Control Points for Focus

From our analysis of the ongoing consolidation, as well as of preferences and top of mind CISO priorities, we expect the cybersecurity sector to consolidate along five key control points:

- **Operating system focus** combines security-related products and services with native tooling and enterprise licenses into a common offering from OS providers such as Microsoft.
- **Cloud focus** brings together extended detection and response (XDR) and CWP in cloud-native forms to monitor data from networks, cloud workloads, servers, email, and other sources. Cloud-first companies and vendors see these offerings as a way to bypass traditional security tools and their related challenges.
- **Endpoint focus** unites previously separate tools and techniques in desktop, laptop, tablet and phone devices, with services taking the place of antivirus software and coordinating with the other systems seamlessly. These services tend to focus on the data first. Vendors include both new entrants (some with rapid growth) and long-established endpoint protection providers that are expanding into detection and response. Like cloud vendors, endpoint vendors increasingly incorporate XDR in their offerings.
- **Network focus** integrates next-generation firewall, detection, and response solutions into secure access services, reaching across on-premises, cloud, and hybrid environments. Some of the most prominent cybersecurity vendors bundle these solutions to expand from the security bedrock of network firewalls to create broader security platforms that encompass networks, endpoints, and more.
- **Identity focus** emphasizes the individual's access to various levels of entry and authorization as a key element and treats the ability to access critical information as central to the system's design and implementation. These vendors benefit from the increasing convergence of user access management, identity and access management, privileged access management, and other categories of corporate identity.

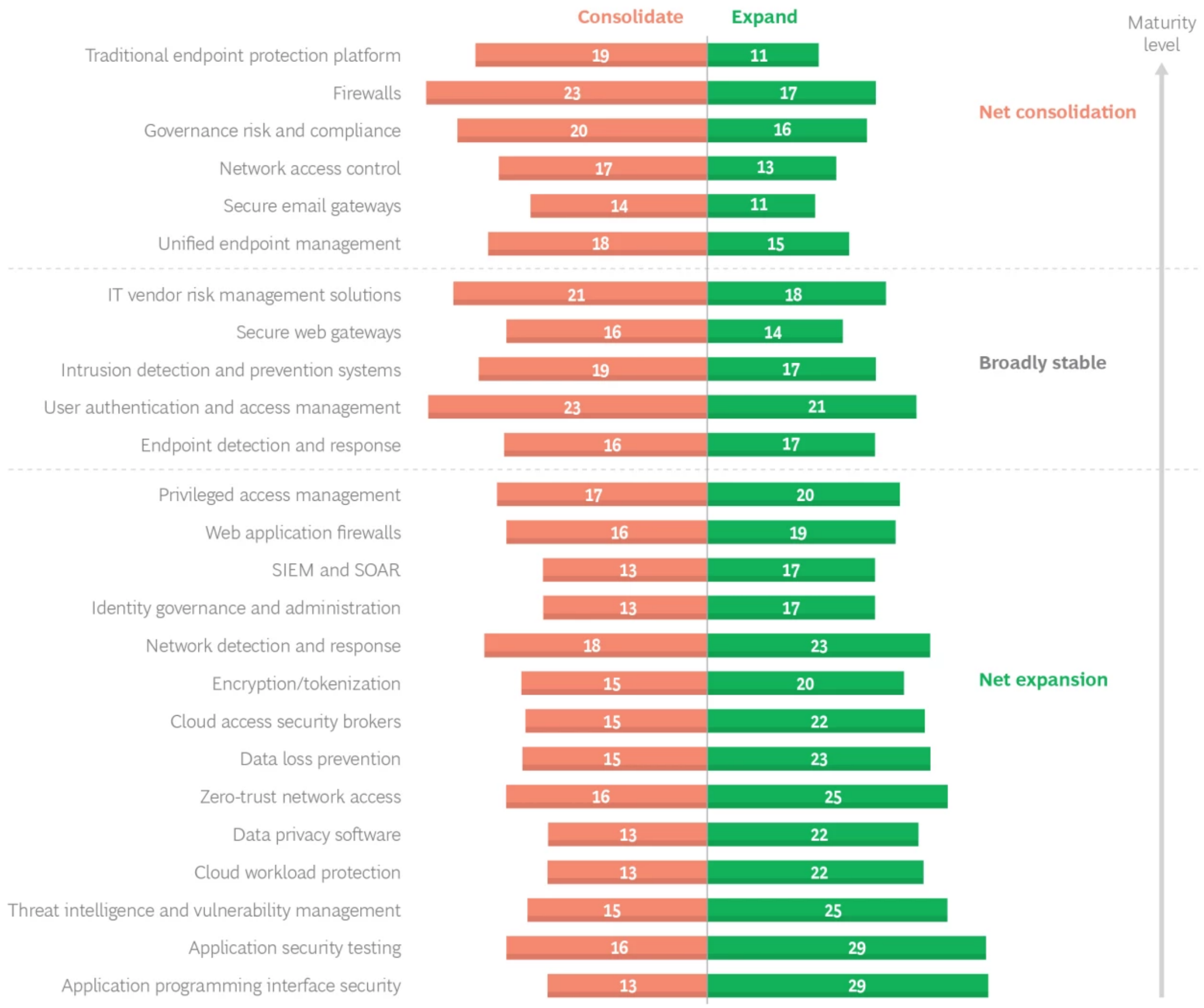
These five control points inspire natural technological and customer solutions from which cyber vendors can easily cross-sell other add-on solutions. Cyber companies that master these control points can use them to develop a high level of competence at a lower cost.

Areas of Diversification

Even as mature cybersecurity technologies face consolidation, experimental and emerging categories are diversifying, with CISOs choosing best-of-breed solutions instead of bundles. When presented with these technologies, cybersecurity leaders are more eager to adopt new tools and add new vendors to their rosters. Examples of such technologies include NDR, AST, and CWP, along with data loss prevention, tokenization and encryption, cloud access security brokers, zero trust network access, data privacy software, threat intelligence and vulnerability management, and API security. (See Exhibit 4.)

Exhibit 4 - Pressure for Consolidation Versus Expansion in Three Types of Cybersecurity Offerings

Q: In which of the following categories is your company looking to consolidate or expand IT systems or suppliers? (%)



Source: BCG and GLG CISO Cybermaturity Survey and Scorecard (n = 600).

Note: SIEM = security information and event management; SOAR = security orchestration, automation, and response.

Over time these solutions may merge with the control points highlighted above. For example, conversations with CISOs indicate that vulnerability management and threat intelligence may fold naturally into broader XDR platforms, creating an opportunity for investors. Point solutions in emerging categories today could become targets for strategic acquirers down the road.

Thriving in the New Cybersecurity Environment

How can cybersecurity leaders protect their organizations against new and existing threats while managing cost pressures? How can cyber vendors help them do this, and differentiate themselves from their competition? Which innovations should investors support?

CISOs and other cybersecurity leaders should adopt the behaviors of best-in-class advanced organizations. The most effective way to do this is to prioritize solutions and organizational improvements with a high ROI. Our survey revealed that 78% of advanced firms regularly measure the ROI of their cyber operation improvements, 68% track enhanced compliance, and 67% analyze their security efforts in terms of business efforts. Similar metrics for unprepared firms are significantly lower: 68% measure operational ROI, 40% track compliance, and 32% pay attention to business outcomes. Unprepared, reactive, average, and proactive companies are also more likely to focus on insurance premiums or other factors that have relatively weak connections to business outcomes.

As they standardize on a few key metrics, CISOs can use the resulting insights to prioritize organizational changes that improve their companies' security posture at lower cost. Enhancements to process and corporate culture can move the needle on security quality even in an environment of budget constraints. CISOs should carefully evaluate new vendors, using an assessment of hard-dollar ROI as a component of the selection process.

Conversely, vendors must demonstrate the ROI of their offerings by showing that they can handle new and emerging threats without expanding total cost of ownership. They may accomplish this through labor savings, reduced insurance premiums, avoided breaches, or increased efficiency in the form of lower impact on business operations.

Investors must either ride the wave of consolidation or focus on solutions that avoid the resulting competitive pressure—by investing either in emerging categories or in niche players. Fast-growing cyber categories will see continued expansion, and category specialists (such as players in the area of managed detection and response) will be relatively resilient to consolidation.

Perhaps the most optimistic result in the CISO survey involved the attitudes of top leaders. A relatively low 53% of CISOs said that they were worried about whether executive commitment at their company was sufficient. To keep top leadership walking the talk, and to meet the challenges of the near future, CISOs must think more broadly about their own activity. They and their teams are not hired just to prevent intrusion. They are increasingly expected to protect and strengthen the digital and overall integrity of the entire enterprise.

Acknowledgments

The authors thank their BCG colleagues Maciej Sniechowski and Pranav Khemka for their contributions to this article.

Authors

Clark O’Niell

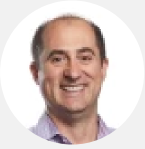
MANAGING DIRECTOR & PARTNER

San Francisco - Bay Area

Varun Khurana

MANAGING DIRECTOR & PARTNER

Seattle



Colin Troha

PLATINION MANAGING DIRECTOR

Washington, DC

Braden Holstege

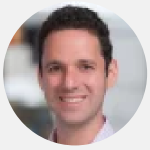
PRINCIPAL

San Francisco - Bay Area

Nadya Bartol

MANAGING DIRECTOR, BCG PLATINION

Washington, DC



Alex Asen

KNOWLEDGE EXPERT

ACC – Boston

Geoffrey Cheung

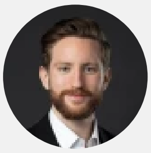
PRINCIPAL

Los Angeles

Matthew Fallon

PRINCIPAL

Washington, DC



Bernhard Gapp

PROJECT LEADER

Silicon Valley - Bay Area

ABOUT BOSTON CONSULTING GROUP

Boston Consulting Group partners with leaders in business and society to tackle their most important challenges and capture their greatest opportunities. BCG was the pioneer in business strategy when it was founded in 1963. Today, we work closely with clients to embrace a transformational approach aimed at benefiting all stakeholders—empowering organizations to grow, build sustainable competitive advantage, and drive positive societal impact.

Our diverse, global teams bring deep industry and functional expertise and a range of perspectives that question the status quo and spark change. BCG delivers solutions through leading-edge management consulting, technology and design, and corporate and digital ventures. We work in a uniquely collaborative model across the firm and throughout all levels of the client organization, fueled by the goal of helping our clients thrive and enabling them to make the world a better place.