Reducing Cyber Risk on a Tight Budget

AUGUST 28, 2023

By Nadya Bartol, Charlie Weinberg, Vijay Pasupathinathan, Chris White, and Nadine Moore

READING TIME: 8 MIN

Many companies are squeezing budgets to free up resources for growth. BCG’s CEO Outlook 2023 showed how the most resilient leaders are funding innovation, sustainability, and other critical projects through tight control of costs. For the Chief Information Security Officer (CISO), this may mean a new era. Increasingly, they are being asked to improve cybersecurity with historically small budget increases. Some may even be asked to spend less. Is it possible to reduce risk in this environment?

Surprisingly, the answer is yes. Implementing a comprehensive cost resilience process can maintain—and often improve—an organization’s risk profile. When optimizing the cyber budget, a CISO will review people, processes, and technology to identify gaps and inefficiencies. Addressing these will allow risks to be reduced while spending is held steady.
In some cases, costs can even be reduced. Consider BCG’s recent work with a mid-sized commercial/retail bank to improve security without increasing costs. Our team conducted interviews and workshops with executive and staff-level stakeholders, analyzed systems and processes, and benchmarked them against best practices in other banks. The project cut 8% from the annual cybersecurity budget while aligning cyber risks with business risk appetite. Key actions and benefits included:

**Exhibit 1 - While Security Remains a Top Priority, IT Professionals Must Now Control Costs**

<table>
<thead>
<tr>
<th>Respondents naming each issue as a Top 3 priority</th>
<th>% change vs. Q4 2021</th>
<th>Rank change vs. Q4 2021</th>
</tr>
</thead>
<tbody>
<tr>
<td>Drive digital transformation</td>
<td>62%</td>
<td>+22%</td>
</tr>
<tr>
<td>Increase security and mitigate risks</td>
<td>50%</td>
<td>-5%</td>
</tr>
<tr>
<td>Enable company growth</td>
<td>49%</td>
<td>+3%</td>
</tr>
<tr>
<td>Control IT spend and costs</td>
<td>48%</td>
<td>+37%</td>
</tr>
<tr>
<td>Improve customer satisfaction</td>
<td>25%</td>
<td>-16%</td>
</tr>
</tbody>
</table>

Sources: IT Buyer Pulse Check 5.0 (December 2022), N = 450; IT Buyer Pulse Check 3.0 (October 2021), N = 676 (APAC excluded).

- Tooling rationalization (more than 5% savings)
- Sourcing optimization (nearly 4% savings)
- Improved operating model (1% to 2% savings)

The increased focus on cost control was highlighted in our 2023 survey of cybersecurity leaders, conducted in association with GLG, an insight network that provides access to expert perspectives. In a difficult economic environment, cyber leaders expect to see annual budget increases of about 4%—in line with vendor price increases—instead of the more typical 8%. However, the pressure to minimize risk remains unrelenting: BCG’s most recent survey of IT buyers shows that improved security remains a Top 3 concern. (See Exhibit 1.)

**Investment as a Benchmark**

Clearly, any cost resilience program must be managed carefully; an organization that cuts corners on cybersecurity is on the fast track to a crisis. Risks continue to proliferate, with ongoing digital transformation increasing the impact of any disruption and attackers deploying new technologies, such as AI.
An important starting point is to look at return on investment. In the BCG survey of cyber leaders, 56% of CISOs in the “advanced” quintile for cyber maturity said they consistently measure cybersecurity ROI; for those in the “unprepared” category, this was just 22%. ROI should provide the yardstick for action as improvements are planned, forcing an alignment between spending and results in the form of reduced risk.

Based on our extensive work with cost resilience initiatives and cybersecurity, we have identified six action areas that can help organizations provide optimal security while controlling costs. Estimated security budget savings from each action are also indicated.

- **Align spending to risk appetite.** This process starts with defining cybersecurity risk appetite, working with business units to quantify the impact of incidents and their knock-on effects. In some cases, it may be useful to compare the organization with peers. CISOs can identify areas where investment exceeds what is necessary to meet the required risk profile and reallocate budgets accordingly. (Estimated savings 5% to 10%)

- **Prioritize the project portfolio.** CISOs need to challenge ongoing investment, which may have been built up piecemeal over years. Ongoing projects must be evaluated, conflicts and overlaps resolved, and priorities decided on a balance of cost and risk reduction. (Estimated savings 5% to 10%)

- **Sharpen security operations.** Review all security operations with an eye to improving operational efficiency. What processes can be automated? Can costs be reduced by changing service level agreements (SLAs)? The aim is to fully align capability and resources with cybersecurity performance requirements. (Estimated savings 5% to 10%)

- **Rationalize tech tools.** Vendors love to sell tools in packages, but over the years this can lead to duplication and waste. Our research shows that many CISOs are looking to consolidate vendors, seeking reduced costs and better security outcomes through improved tool integrations. This requires analyzing opportunities for tool and capability consolidation and renegotiation, including across the technology stack. Custom products, tools with marginal added benefit, and those that may be redundant all must be put under the microscope. Tool vendors must clearly demonstrate the ROI of their offerings, for example, by showing how they can save labor, cut insurance premiums, combat new threats, avoid incidents, or reduce the efficiency impact on business operations. (Estimated savings 5% to 10%)

- **Review sourcing strategies.** After determining which tools, services, and other capabilities are necessary to meet the organization’s goals, security leaders need to optimize the purchase process, vendor incentives, and performance expectations. SLAs and in/outsourcing decisions should be reviewed to identify ways to maximize cost efficiency while meeting performance expectations. (Estimated savings 3% to 10%)

- **Improve the operating model.** To enhance security operations, CISOs can optimize staffing and organization issues by looking at overlapping roles, duplicative processes, who makes decisions, and the span of control. They can also ensure that staff are spending time on the tasks that drive the biggest risk reductions. (Estimated savings 1% to 5%)

**Develop a Custom, Structured Approach**
Although IT security leaders may be keen to get started, we urge a moment of caution. A rigorous approach must be deployed to maximize cost savings without damaging the organization’s cybersecurity risk profile. In addition, each organization has a distinct cyber risk profile due to differences in technology, threat landscape, and business priorities; there is no one-size-fits-all method to protect against risks.

The process should begin with a short, one- to two-week diagnostic to identify action areas with the most significant possible savings, followed by selecting the method that best addresses those areas. Multiple methods will sometimes be deployed; if so, they must be carefully sequenced.

We have identified five methods that can be deployed to create a roadmap for cutting costs while maintaining security.

- **A cyber tool health index** and inventory finds gaps in implementation, areas where security can be improved, and tools that are under-deployed or duplicative and can offer cost savings. The result is an optimized tools budget with a much clearer view of cost-effectiveness. Savings from reduced use of legacy tools can be recycled into buying new ones in emerging areas, such as open-source software or artificial intelligence. It is essential to monitor tool costs and usage on an ongoing basis to ensure budgets are being spent effectively.

- **Optimizing cyber sourcing** is another targeted approach. This starts with refreshing the cybersecurity sourcing strategy. This may mean identifying new vendors with more competitive pricing, supporting contract negotiations with existing or new vendors, redefining SLAs to match risk appetite, restructuring vendor performance incentives, or terminating relationships with vendors whose products are no longer needed. Again, savings can either be deployed to reduce overall spending or reallocated with new vendors to drive down the risk profile.

- **Zero-based budgeting (ZBB)** goes further, asking fundamental questions about the cost base and the value delivered. Zero-based budgeting is a proven process that rigorously aligns spending with strategic priorities, and in this context it creates a plan that will impact multiple cost-saving areas. ZBB drives operating model improvement, portfolio optimization, better sourcing, and alignment to risk appetite.

- **Systematic improvement** achieves better outcomes by looking at deeper, organizational issues and aims to create a lean but highly effective cybersecurity organization. An example would be adopting agile practices at scale, increasing organizational execution velocity, and redesigning the cybersecurity operating model. Leadership is essential here; the new operational model must enable a clear link between cyber risk strategy, the teaming model, and process execution. Increased agility is a clear organizational asset when responding to the fast-changing threat landscape.

- **BCG’s Cyber Risk Quantification (CRQ)** takes a strategic approach, battle-tested across a wide range of organizations with highly varied risk profiles. It looks at the likelihood of attacks and their possible impact to deliver a blueprint for action driven by ROI, which our research shows is typically deployed by companies that are most mature in managing cyber risk. As shown in Exhibit 2, BCG’s CRQ process bases cybersecurity investment on the amount of cyber risk it reduces.
The output from CRQ is a prioritized list of actions that can range across the entire cybersecurity operation, from sourcing strategies to improved workflow—providing a foundation for enhancing the risk profile while still containing costs. They focus management attention on activities that yield big savings rather than those that are quick or easy.

Whatever the approach, the final, and critical, step in the process is preparing and implementing the cyber cost resilience program. A short-term, cross-functional team is required to manage execution, pushing through the quick wins while establishing a change management plan for processes that require a more complex organizational response. Throughout the process, measuring the impact on costs is essential to validate objectives.

Across many firms, cost control is the new imperative. The BCG CEO Outlook 2023 showed that company-wide savings are being invested not just in innovation and sustainability but in up-skilling, improving supply chains, and many other projects that require additional resources in turbulent times. As such, the cost pressures on CISOs are unlikely to ease despite increasingly potent cyber threats to the organization.

Yet it is possible to reconcile these imperatives—indeed, skillful management can contain costs while enhancing security if suitable methodologies are implemented. Even when budgets were more generous, the steps outlined in this article were beneficial; in today’s more challenging times, they are essential.
Authors

Nadya Bartol
MANAGING DIRECTOR, BCG PLATINION
Washington, DC

Charlie Weinberg
PLATINION ASSOCIATE DIRECTOR
Atlanta

Vijay Pasupathinathan
PLATINION PRINCIPAL, CYBERSECURITY

Chris White
PLATINION PRINCIPAL, CYBERSECURITY
Washington, DC

Nadine Moore
MANAGING DIRECTOR & PARTNER
Chicago

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.

© Boston Consulting Group 2024. All rights reserved.

For information or permission to reprint, please contact BCG at permissions@bcg.com. To find the latest BCG content and register to receive e-alerts on this topic or others, please visit bcg.com. Follow Boston Consulting
Group on Facebook and X (formerly Twitter).