ARE YOU SPENDING ENOUGH ON CYBERSECURITY?

By Alex Asen, Walter Bohmayr, Stefan Deutscher, Marcial González, and David Mkrtchian

If you have any technology budget responsibility, it's a question you are going to hear—a lot. "Are you spending enough on cybersecurity?" It's asked by customers, shareholders, regulators, board members, and executives wondering aloud if there's a price at which peace of mind can be purchased.

Any leader—including CEO, chief risk officer, chief information security officer, even chief financial officer—who is asked the question will find it tremendously difficult to answer. A "yes" will leave you precariously positioned if—or when—your cybersecurity falters. Say "no," and you'll likely trigger a scramble to purchase something—anything—that can reverse that answer and protect you from the perception of negligence. No shortage of vendors will step up to oblige with a plethora of technologies, products, services, promises. But there's no guarantee that any of these "magic bullets" will really meet your organization's needs. And if you move forward without proper diligence, you risk spending too much on the wrong thing and proliferating the false belief that security can be ensured simply by meeting some budget benchmark.

The best response: answer the question with questions. That way, you'll hone your understanding of the landscape and begin to build cybersecurity competence—and cyberresilience—across your institution. Then you can make an informed decision about what's right for your organization.

How Much Is Enough?

No surprise, cybersecurity is expensive and becoming more expensive.

As the world becomes ever more reliant on technology, and as cybercriminals refine and intensify their attacks, organizations will need to spend more on cybersecurity. Indeed, Gartner reports that average annual security spending per employee doubled, from $584 in 2012 to $1,178 in 2018. Some of the leading banks and tech companies have total annual cybersecurity budgets that exceed half a billion dollars and continue to grow.

If you are thinking about solving your cybersecurity challenges by purchasing new technology products and services or increasing security staff, you are likely looking for guidance about how much spending to allocate. But it's hard to compare an individual company's spending against any benchmarks. Some of the leading voices in the industry prescribe very different approaches to calculating spending on cybersecurity. (See Exhibit 1.) These differences reflect some fundamental truths, misperceptions, and unknowns about cybersecurity at this stage of the game.

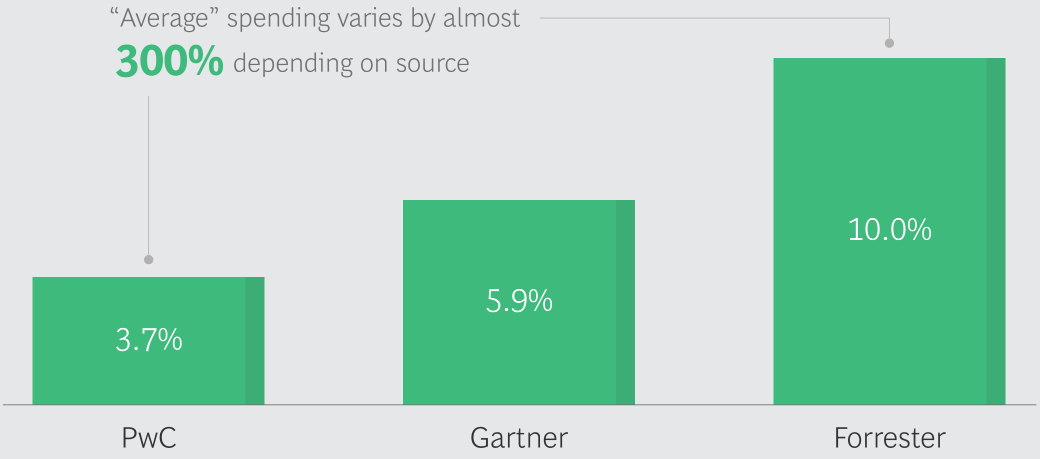
Existing regulations offer no specific guidance to help you understand what you are actually spending on security. There's also no common definition or accounting methodology to lend clarity. This challenge is unlikely to be resolved given that cybersecurity spending is often implicitly distributed across multiple departments' budgets. Indeed, cybersecurity is inherently transversal. It requires partnerships between the IT, risk, fraud, physical security, compliance, and legal functions; the lines of business; and others. Some of the most effective security-related spending will never be part of the explicit cybersecurity budget. For example, high security standards will drive up procurement costs, because the least expensive supplier might not have the required security capabilities and certifications. High security standards can also increase technology costs: secure software development methods require more developers, for example, and using strong encryption for web traffic requires more servers. And security can drive up HR costs by requiring more-thorough background checks and training, or a head-count-intensive review process in which two sets of eyes must be applied to all key business processes.

Given these variables, determining the appropriate spending on cybersecurity should come only after a careful assessment of your organization's current—and future—needs and capabilities.

What Are the Right Questions to Ask?

Although, currently, some chief information security officers (CISOs) reportedly enjoy unlimited budgets that give them access to alluring and expensive new technical solutions, no organization has a boundless

Exhibit 1 | No Standard Benchmark of Cybersecurity Spending Exists



Average security spending as a percentage of IT spending according to three different benchmarking sources

Sources: *The Global State of Information Security Survey,* PwC, March 10, 2017; *IT Key Metrics Data 2017,* Gartner, December 12, 2016; 2017 Tech Budget Benchmarks, Forrester Research, March 28, 2017; BCG.
Note: Measuring security spending as a percentage of IT spending is a common metric because technology intensity is often a key driver of security need. This is not to imply that security is solely an IT issue or that security spending is limited to the IT budget.

capacity to implement and operate simultaneous improvements. Such a “give it our all and then some” approach to technology distracts resources from more effective organizational and cultural improvements, and can leave an organization less secure.

Security is not a discrete layer to be piled onto the existing business. CISOs and other executives must collaborate closely to embed security in their organization’s culture and process. More than 70% of breaches are caused by failures on the part of people and processes, so getting these organizational elements correct is crucial. (See “Building a Cyberresilient Organization,” BCG article, January 2017.)

Asking yourself the following three questions can help. (Exhibit 2 summarizes the questions—and how to prepare to answer them.)

What is our risk appetite? One large government-owned bank in the Americas decided that its public mandate required near-perfect system availability, even in the face of a cyberattack. With this low risk appetite, the bank was willing to invest $250 million on high-performance backup systems—much more than other organizations of similar size would spend. Still, it’s important to bear in mind that even near perfect comes with residual risk that no amount of spending can completely mitigate.

Most of the time, an organization must be prepared to accept a level of risk that is not near perfect—that is, in fact, quite a bit less than perfect. For example, after suffering a suspected breach, a US industrial manufacturer contracted with a technology vendor to ship pallets of expensive next-generation firewalls to every location where the manufacturer operated. At certain locations, the firewalls were needed and used. But it became apparent that they were not appropriate everywhere: the

EXHIBIT 2 | A Cheat Sheet for Your Next Cybersecurity Budget Review

Questions that boards of directors and C-suites should ask	How a CISO or other leader should prepare to answer
What is our risk appetite? Is this budget correctly targeted and in line with our risk appetite and cybersecurity maturity ambition level? • Are the individual assets (data, system, or process) that we are protecting valuable enough to justify the investment or are there other assets that should be prioritized instead? • Is our ambition level in line with our business strategy?	Develop an asset inventory. At early maturity levels, take a pragmatic approach to focus on inventorying and protecting the most critical assets. The board must set your risk tolerance and ambition level, which should then inform a decision process on which assets and threats to prioritize and how much budget to request.
Where will our investment be most effective? Is our understanding of our risks and capabilities sufficient to assess where our spending will be most effective? • Are we mainly aiming for regulatory compliance or for risk reduction and business enablement? • Do we have adequate granularity, currency, and accuracy to prioritize spending?	First, align your program with a relevant maturity framework.[1] Then, gain an honest view of your current position and a target maturity informed by the board’s risk tolerance and ambition level. Investments can then be ranked and put on a roadmap according to their ability to move you from your current state to the target state.
How do we make our investments work? What do we know about the capabilities we are seeking to purchase, and how do we make our initiative successful? • Are these capabilities that we already have within our existing tools and solutions? • Will these capabilities be effectively deployed and managed by existing staff?	Conduct an inventory of unused features among your current security tools. If a new tool overlaps but is better, consider the possibility of decommissioning the old tool. Always have a plan for how new investments will be managed and integrated into existing processes. If it requires new hiring, have a plan for that too. Ensure that redundancies are by design, not chance.

Source: BCG.

[1] For instance, ISO 27001 or the NIST Cybersecurity Framework (CSF).

company had a long tail of very small offices that were not critical for company operations, did not hold sensitive data, and were sufficiently separated from the critical systems. The expensive firewalls, with their high management overhead, were not the right solution for these small offices. Rather, the right solution was to accept the possibility of an inexpensive breach of noncritical systems rather than investing millions to protect low-value assets.

These examples demonstrate three requirements: First, develop an asset inventory so that you know what you are protecting; this is a crucial step in ensuring that security resources are deployed where they are most needed. Second, with that understanding established, define a risk appetite in order to instill strategic direction in your security-spending decisions. This is a key responsibility of the board of directors. (See *Report from Davos: Board Oversight of Cyberresilience*, BCG and World Economic Forum report, January 2017.) And, third, to the degree possible, assess the financial impact of the cyberattacks you might face; this is essential to determining how much to invest to mitigate them. This third requirement is a difficult undertaking, as the next question explores.

Where will our investment be most effective? Getting the most value from your cyber investments requires understanding the risks you are facing, your risk appetite, and the defensive capabilities you currently have. The gap between risks and capabilities is where investment must be targeted. This process is effective only if risks are quantified and capabilities are accurately gauged, however. Targeting gaps is only a first step: you also need to make sure you are spending in ways that will sustain your existing capabilities as the environment evolves. Otherwise, you'll just create new gaps.

Cyberrisk, compared with other kinds of risk, like fire or flood, is a new and evolving field, with limited valuable actuarial data to rely on. (This is a serious challenge even for the insurance industry.) It's also true that given the pace of technology change, past data is a poor proxy for future cyber mayhem. Put differently, you never have enough relevant data because the threat surface changes as adversaries and computing platforms evolve. For now, at least, making sound decisions regarding cyberrisk must involve both reducing ambiguity to a bare minimum and accepting that some degree of ambiguity is unavoidable.

That is illustrated by the experience of one large health care provider, which originally assessed its cybersecurity risks on an ordinal scale—high, medium, and low. Such assessments are a good start, but ordinal scales are insufficient because one person's "high" risk can be a 50% probability while another's can be 70%. Those two figures have fundamentally different implications for how much to invest to mitigate risk. You need to go further by attaching numerical probabilities and eventually monetary estimations to the risks, lending transparency and commonality. Numerical reasoning provides decision-making clarity, and order-of-magnitude accuracy is both useful and possible. It's hard to make an ROI decision as a business executive without being able to compare apples to apples and dollars to dollars.

It's true that unforeseen and unimagined dangers lurk, but decision makers cannot be paralyzed by the specter of these possibilities. They must move forward with the best information and best instincts they have. Then, they can turn to building the organizational resilience necessary to address and recover from the unknown unknowns.[1]

Once you understand the possible risks and their impact on your enterprise, you can start to measure how much risk is mitigated by existing capabilities and where the gaps are. Here, it is crucial to understand not merely what capabilities you have on paper but how effectively implemented and operated those capabilities actually are. The difference between what is believed to exist and what is providing operational value can be wide.

One large consumer packaged goods company that had been relying on an external auditor to assess its cyberrisk and maturity discovered—after a breach—that its auditors had repeatedly mismeasured its capabilities. Because security audits often seek only to ensure compliance with regulations, one of the most valuable investments a company can make is to get a holistic second opinion regarding its actual maturity: an assessment based on business risk, not mere compliance. Real cyberresilience requires much more pressure testing and business understanding than is contained in a checklist for a compliance audit. (See *Cybersecurity Meets IT Risk Management: A Corporate Immune and Defense System*, BCG Focus, September 2014, updated October 2018.)

How do we make our investments work?

Once you've identified the biggest gaps between your risk and your capabilities, you know where to spend. Next, you must determine how to spend—but don't assume that this necessarily means you need to buy something new.

In our experience, organizations rarely use all the security tools and features they have purchased. For example, a professional services company was planning to purchase a system that would allow it to test email attachments in a safe, "sandbox" environment before they could harm company computers. In the middle of the planning process, the company hired a new CISO, who discovered that the e-mail security gateway the company already owned had an unutilized feature for sandboxing. Her staff enabled the feature and gained the functionality, with minimal added cost or management complexity. Before embarking on ambitious investments or falling victim to the shiny-new-object attraction, it is paramount to verify that the capabilities you seek are not already in hand.

Some tools or functionalities will indeed be new to an organization, of course. In those cases, it is important to consider the implicit cost of deploying, running, and managing a new solution. Some security solutions are truly turnkey—add-ons to an existing tool that leverage a similar user interface, for instance. (Even those, because they induce change, can have hidden process costs.) But many are not. For example, one small financial institution invested in a state-of-the-art monitoring solution and threat intelligence feed—only to find that its existing staff did not have the capabilities and expertise to integrate these solutions into the security workflow. New offerings often require existing security staff to climb a steep learning curve; they might even require hiring more staff. This is usually an expensive proposition given the massive talent gap in the field of security. (See *How to Gain and Develop Digital Talent and Skills*, BCG Focus, July 2017.)

Another cost element that is often overlooked when making purchasing decisions: the productivity impact a new tool can have on company productivity—a cost that's exacerbated if the tool is poorly implemented. One corporate office, for example, introduced a solution for data loss prevention that, as a side effect, drastically reduced data transfer rates and system stability. In this instance, the money saved by implementing the tool without proper field testing was trivial compared with the negative effect on the business.

Finding the resources to run a proof of concept or pilot can pay big dividends. As you move into the implementation phase, it is important not only to document the used features of the new tool but also to inventory unused features in case you need to enable them later. Some leading organizations even log missing features so that they can nudge the vendor to implement them in a later iteration.

But How Much Is Too Much?

Regardless of what happens with the budget, it will still be necessary to monitor for misspending and overspending.

We see many companies working to optimize their security portfolio spending to make each dollar deliver greater value, by utilizing all the features of existing solutions and adopting new approaches, such as security automation and managed security services. One company was making a significant investment in identity and access management (IAM; the ability to ensure that the right people have the right access to the right assets). Benchmarking showed that this organization was, in fact, spending more than its peers. But upon further review, we found that this spending behavior signaled not that IAM was a priority, as one would expect, but that the IAM capability was immature and neglected and thus a source of inefficient overspending. The firm had a large team of people manually conducting routine administrative IAM processes that can, and should, have been automated. By investing in consolidated systems and automated processes, the firm increased its IAM maturity and reduced costs.

And there are other ways to free up cash for new security investments while working within an existing budget—standard cost-saving levers like renegotiating license costs, for instance, and consolidating duplicative functions. But when it comes to security, redundancy is often a good thing, so you need to distinguish between the extra processes and solutions that add no additional value and those that lend useful redundancy or limit the risk that is inherent to monocultures, which rely on a single solution and thus are less resilient.

Overspending is as important a consideration as misspending. You are overspending on security when you simply pay too much for what you get (a procurement problem, for instance) or if you are providing a higher level of protection than your risk tolerance mandates. In this case, reducing the security budget is appropriate, but companies that do this need to stand by the risk appetite that they have defined. They must understand their risk and accept certain interruptions or breaches not as failures of management but as the strategically calculated cost of doing business. This requires that senior managers commit to respect the thresholds they have set; when breaches occur, they should not punish a CISO for missing higher expectations that were not articulated, agreed upon, and funded.

At the most advanced maturity levels, companies treat minor cybersecurity incidents as opportunities to raise awareness and sharpen response and recovery procedures that will be needed in the event of a major breach. For example, when one large bank identified hackers attacking its systems, it monitored their activity in order to learn from it rather than moving immediately to stop them; only once the attackers had stolen more than $10 million did it try to expel them. (This kind of threshold should be agreed upon up front, but the actual number should be well guarded; otherwise, an organization with a $10 million limit will see a lot of attacks leading to damages of only $9.5 million.)

As the example shows, be wary of complacency. It's necessary to continuously improve security just to keep up with the bad guys who themselves are always innovating. This need not engender misspending or overspending, though. A well-run security department can enter a virtuous cycle in which the efficiency-based cost savings generated by new investments free up money for the next round of investments.

Who Has the Answers?

We maintain that "how much are you spending?" is not the key question to ask when assessing cybersecurity but concede that it's a ubiquitous one. When it's asked, and it will be, most companies will turn to their CISO, who may or may not be able to answer it. Ultimately, though, the board of directors and C-suite are accountable.

Whatever your role—CISO or member of the board or C-suite—you need to be prepared to answer the question. Once you have asked and answered the truly necessary questions (summarized in Exhibit 2), you can develop a risk-based security strategy that you can stand by. You will be prepared to justify, with robust maturity and risk assessments, your spending decisions, whether they involve decreasing or increasing security spending or maintaining a level less or more than the median among your peers.

The specter of a cybersecurity incident does not negate the need to be a judicious steward of company resources, and security spending is not a good proxy for security effectiveness. Yes, you will have to devote some of your budget to this issue, but by asking the right questions you will target your spending wisely rather than feeling pressured to simply throw money in the general direction of the problem.

NOTE

[1] *How to Prepare for the Unknown Unknowns,* World Eonomic Forum, January 2015.

About the Authors

Alex Asen is a lead knowledge analyst in the Boston office of Boston Consulting Group. You may contact him by email at asen.alex@bcg.com.

Walter Bohmayr is a senior partner and managing director in the firm's Vienna office. You may contact him by email at bohmayr.walter@bcg.com.

Stefan Deutscher is an associate director in BCG's Berlin office. You may contact him by email at deutscher.stefan@bcg.com.

Marcial González is a principal in the firm's Bogota office. You may contact him by email at gonzalez.marcial@bcg.com.

David Mkrtchian was formerly a consultant in BCG's Los Angeles office.