AlixPartners

Digital
MARCH 2018

CYBERSECURITY

What CEOs need to do before the next threat

It's a safe bet that cyberrisk is here to stay. It's also likely that its looming threat will multiply—maybe exponentially—as we dive deeper into the digital age.

The good news is that governments, international regulatory bodies, and think tanks now recognize how destabilizing the threat can be to companies, markets, and even whole societies. The bad news is that even forward-looking regulations and massive investments in new technologies run the risk of playing catch-up to hackers' even smarter tricks.

As cybersecurity becomes more integral to the new economic and social system, businesses not only need to build the sturdiest IT security infrastructure they can, but also address the human component. The behavior of every single employee is critical—and it starts with the CEO.

THE ROLE A CEO SHOULD PLAY

Modern CEOs have to be knowledgeable about cybersecurity. Controlling, protecting, and carefully using information will become only more critical as we hurtle into a more deeply interconnected world. The responsibility for safeguarding that intelligence starts at the top.

At a minimum, a CEO should examine the company's organizational design, tactics, and overall strategy, and then answer the following questions:

ORGANIZATIONAL DESIGN

- Are all of my direct reports involved in cybersecurity processes and decisions? What kind of involvement does the C-suite have?
- Do we have an active cybersecurity advisory board?
- Do we have the right skills in place for a holistic approach to cybersecurity?

TACTICS

- Do we take a risk-based or an IT-centric approach to cybersecurity?
- Do we have clear understandings of what cybercapital is at risk and how the cybersecurity strategy would proactively and reactively manage that cybercapital?
- In the evaluation of cybersecurity risks, are all department heads involved so as to ensure clear prioritization of the business assets and related quantification of the business impact?
- What kind of advance techniques—like artificial intelligence and machine learning—do we use to calculate the likelihood of internal and external threats?
- Is the board involved in setting the level of the company's cybersecurity risk appetite?

STRATEGY

- Is the cybersecurity strategy defined and regularly updated to align with our actual business risk and our related-risk appetite?
- Are our cybersecurity investments justified by resulting in risk reduction?
- Do we have the right tools and processes in place to dynamically evaluate our cyberrisk level in case of boundary changes, including different architecture, systems, applications, threats, etc?

Addressing the organizational design questions is especially important, but unfortunately, those answers often get sidelined. In our experience, business leaders tend to assume that their biggest cybersecurity challenges are technological. However, many of the challenges are actually organizational (see box, "Glitches in the system").

Glitches in the system: how your current setup may be flawed

- The enterprise as a whole fails to take responsibility and relies instead on a classic bottom-up approach to cyberthreats driven only by IT.
- The IT department has sole discretion to decide where to invest and asks for budgets without clearly quantified justifications.
- The business operates with a tick-the-box approach to managing cyberrisk.
- There is no chief information security officer (CISO) at all, or the CISO is reporting to the chief information officer (CIO) rather than the CEO, the chief risk officer (CRO), or the chief operating officer (COO).
- The company fails to recognize that IT security is just one part of information security.
- The company conducts only partial—or, worse, misguided—evaluation of business impacts.
- The company does indeed allocate capital on the basis of various risks and yet does not include an allocation to cyberrisk.
- The board is not engaged in these efforts and does not help define the company's risk appetite.
- Cyberrisk is usually lumped in with IT risk and not integrated with enterprise risk management.

"In our experience, business leaders tend to assume that their biggest cybersecurity challenges are technological."

Fortunately, that means CEOs may have more power than they think for improving their cybersecurity measures and truly integrating them into their businesses. But where to start this year? We recommend that CEOs focus on taking the following six steps:

1 TAKE FULL OWNERSHIP IN THE C-SUITE

CEOs should treat cybersecurity not as an IT issue, but as a top-down issue that needs to be managed by a team of key people, including the chief risk officer (CRO) (for a risk management point of view as well as metrics and risk analysis), chief financial officer (CFO) (to help the company adhere to regulatory requirements and analyze the economic capital implications and allocations), and chief operations officer (COO) (for embedding the approach into IT operations and the HR culture of the company). The CEO is responsible for clearly outlining the policies, processes, and roles and responsibilities of all these key stakeholders.

2 REVISE THE ORGANIZATIONAL STRUCTURE

Responsibility for setting the right internal structure lies with the CEO, and deciding where the chief information security officer should sit is a big part of the equation. For example, the CISO could stay inside the IT function, but has to be closely linked to the CRO too, and be an active member of the top management team.

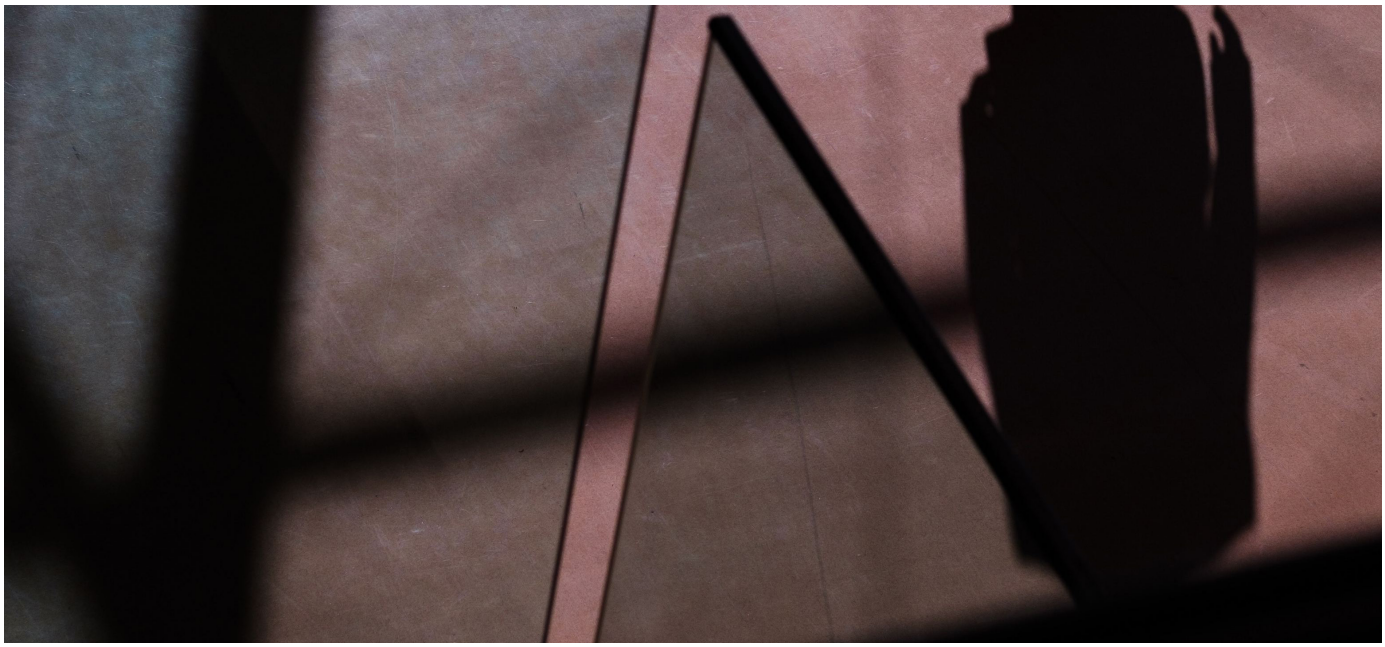
Additionally, the CEO should form a cybersecurity advisory board that will enable executives, security, and IT managers to discuss fundamental security issues, challenge current security measures, and include their business judgments (see box, "Introducing the cybersecurity advisory board"). Finally, the CEO should also ensure that the company makes distinctions between security governance, design, implementation, and operation.

3 BUILD A CYBERSECURITY DASHBOARD

The CEO and the cybersecurity advisory board must have access to detailed, real-time data about the company's level of cybersecurity risk, including any variations in the level of risk that come with changes in the company's business processes and applications, IT infrastructure, third-party relationships, and overall cyberthreat environment. That information could be delivered through a cybersecurity dashboard that uses key performance indicators and key risk indicators to provide the CEO with real-time alerts.

4 CONDUCT A THOROUGH RISK ANALYSIS

A risk-based approach to cybersecurity should start with an evaluation of the potential financial, reputational, and compliance-related impact on business processes and assets in case of a data confidentiality, integrity, or availability loss. The CEO should decide who the stakeholders should be for this evaluation by choosing the right business leaders, business process owners, and data owners to involve. It's also essential to have clear mapping for business process, business assets, and technical assets, making sure to classify them by risk, determining the critical processes and assets. This is the key connection between the business and cybersecurity, because cybersecurity management should be linked directly to the importance of company information.



5 STRATEGICALLY ALLOCATE CAPITAL AT RISK

As the CEO's cybersecurity role becomes more strategic, he or she will need to examine the company's cybersecurity risk appetite and any consequent trade-offs. For any processes or business assets that have risk levels above the company's risk appetite, the company should outline which mitigation activities—including process, people, and technology—would be appropriate. It's up to the board and the CEO to define the strategic allocation of "capital at risk" needed to mitigate cyberrisks below the risk appetite level. Next, the company can design a detailed plan and investment—including capital expenditures and operating expenses—in which each cybersecurity investment is prioritized and justified by reduction in business risk, also known as cybersecurity return on investment.

6 USE AI AND MACHINE LEARNING

Management should consider using artificial intelligence (AI) or machine learning techniques to improve its analysis and evaluation of the most-critical threats for specific markets and geographies. Sharing some of that data with peers in the market (by way of a sector, national, or multinational "Computer Emergency Response Team") would extend the company's capacity to effectively and efficiently respond to and recover from attacks.

HOW TO MANAGE CYBERSECURITY VERSUS BUSINESS TRADE-OFFS

As with everything in life, building a high-performing organization these days often means sustaining certain critical trade-offs. The more you innovate digitally, the more cyberrisk you underwrite. The more digital convenience you offer, the more cyberinsecure you become. If a CEO wants to have foolproof cybersecurity, frankly, the only option is to operate the business in an underground bunker.

To build a strong cybersecurity program in the real world, here are a few pragmatic recommendations:

- The CEO should set competitive strategies across all service lines and consider the implications for both the business and operating models on the basis of the optimal allocation of resources so as to strike an ideal balance between these new kinds of risks and opportunities. Such a strategic allocation should be steered by the CEO and involve heads of business units, the CRO, the CFO, and the COO. And of course, it should be supported by the CISO.
- Cybersecurity is all about measuring the right areas, correctly. To optimize trade-offs, you have to understand them from an objective point of view. And you must measure them comprehensively, because they will entail both technological and business costs, including tangibles (loss of revenues, extra costs, potential fines, and liabilities) and intangibles (loss of brand value and reputation). Also, forget about historical-series-based statistical approaches. From a risk management perspective, we're moving into uncharted waters. And the first to navigate the rough seas will gain an incredibly valuable competitive advantage.
- Once you've carefully evaluated your trade-offs, you should manage the tail risks you simply cannot afford to bear (overinvest in safeguarding against them because they simply must not happen) and insure the consequences you can afford to endure. And finally, decide tactically—on the basis of economic convenience—on all the others.
- Ultimately, to build the strongest cybersecurity program possible, that program has to be grounded on the human component of your business. And the process begins and ends with the CEO.

INTRODUCING THE CYBERSECURITY ADVISORY BOARD

The cybersecurity advisory board should provide a channel of communication between security experts and the business to accelerate critical projects that require interdisciplinary contributions such as that proposed by the European Commission's General Data Protection Regulation or insider risk reduction. The board should serve in a strategic risk reduction function and reduce reputational damage in the event of a security incident by ensuring that company executives are directly engaged in security risk management. Typically, a board would:

- Hold quarterly meetings chaired by an independent expert. A two- or three-hour meeting enables issues to be understood and discussed in depth.
- Comprise—at least—the CEO, CIO, CFO, COO, CISO, general counsel, risk team, and audit team as well as human resources. Ideally, it should also include independent experts from the sector and midlevel directors from the business.
- Focus on an agenda that discusses risk, continuous improvement, and the operating model.
- Ensure that cross-functional responsibilities for data privacy and security get discussed, understood, and assigned.

AlixPartners

CONTACT THE AUTHORS:

Claudio Scardovi (cscardovi@alixpartners.com) and Lorenzo Grillo (lgrillo@alixpartners.com).

FOR MORE INFORMATION CONTACT:

Claudio Scardovi
Managing Director
+44 20 7098 7615
cscardovi@alixpartners.com

ABOUT US

For nearly forty years, AlixPartners has helped businesses around the world respond quickly and decisively to their most critical challenges – circumstances as diverse as urgent performance improvement, accelerated transformation, complex restructuring and risk mitigation.

These are the moments when everything is on the line – a sudden shift in the market, an unexpected performance decline, a time-sensitive deal, a fork-in-the-road decision. But it's not what we do that makes a difference, it's how we do it.

Tackling situations when time is of the essence is part of our DNA – so we adopt an action-oriented approach at all times. We work in small, highly qualified teams with specific industry and functional expertise, and we operate at pace, moving quickly from analysis to implementation. We stand shoulder to shoulder with our clients until the job is done, and only measure our success in terms of the results we deliver.

Our approach enables us to help our clients confront and overcome truly future-defining challenges. We partner with you to make the right decisions and take the right actions. And we are right by your side. When it really matters.