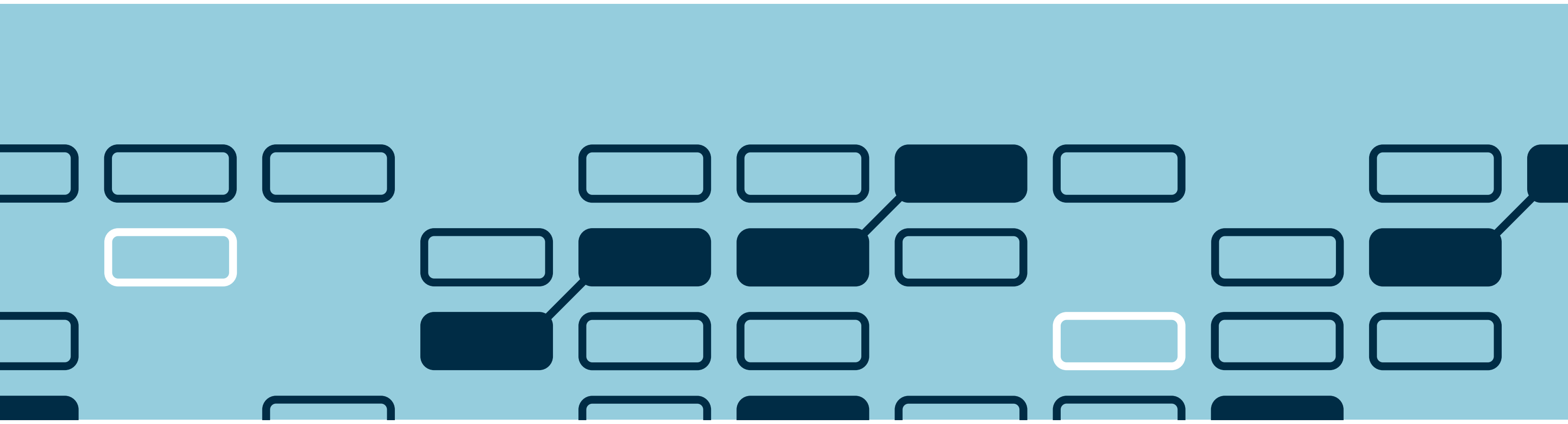
AlixPartners
when it really
matters

DIGITAL

MARCH 2016

Cybersecurity and risk management: lead from the c-suite



Cybersecurity risks have caused concern ever since 1969, when the first nodes of data were transmitted through the precursor to the World Wide Web. The World Economic Forum[1] now ranks those risks as the fifth-greatest threat to global stability—bested only by war, drought, climate change, and widespread unemployment. The relentless evolution of cybersecurity threats should prompt corporate leaders to deal with them from the c-suite rather than leaving their risk management to the information technology (IT) department.

Today's increasing reliance on information technology and industrial control systems in both the private and public sectors means cybersecurity risks must be addressed like any other business risk—and integrated into an enterprise-wide risk management framework. Many top management teams still view cybersecurity as too technical an issue to manage at the executive level, but it's more vital than ever that procedures for handling such concerns get incorporated into an overall risk management regime.

It's more than a question of semantics. Enterprise risk management frameworks fit different standards and definitions as stipulated by international certification bodies and national regulators for dealing with a vast array of legal, compliance, and international certification issues. Those frameworks, standards, and definitions in turn affect how litigation, insurance, and organizational liability get determined.

[1] World Economic Forum, The Global Risks Landscape 2015," accessed January 20, 2016, http://reports.weforum.org/global-risks-2015/#frame/20ad6.

> “Every company in a connected world faces threats that can imperil the very lifebloods of a modern business: its data and its brand

Most important is the fact that organizations that apply globally recognized enterprise risk management standards and practices to cybersecurity issues are offering their clients and customers the most thorough level of protection—one that reflects best practices.

The scope of cyber risk management and best practices has evolved beyond mere ‘prevention’ of cyberrisks; it now encompasses responsibility for the detection of and the capability to respond to cybersecurity incidents. And that detection and that response require a more nuanced approach to risk management.

Every company in a connected world faces threats that can imperil the very lifebloods of a modern business: its data and its brand. And the constant increase in cyberattacks means it’s not a matter of ***whether*** one occurs. One will ***definitely*** occur—sooner or later.

A company’s response to making cybersecurity preparations has implications for the entire organization. Top management must be fully engaged so as to make proper use of the people, process, and technology controls that address the threats while incorporating the goal of protection into the business’s overall aims.

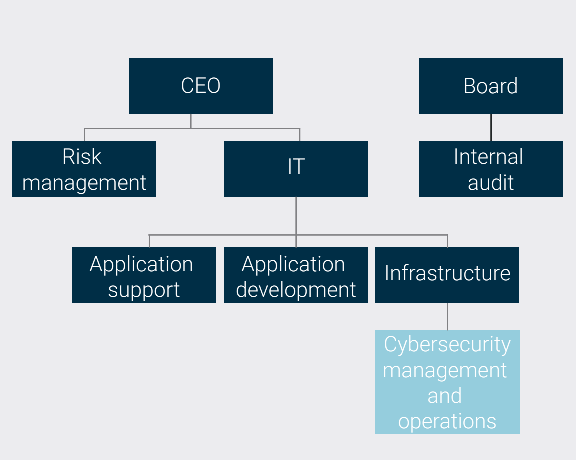
Several models of effective cybersecurity risk governance plans are available that can fulfill the requirements of effective overall enterprise risk management. Certain guidelines help do that effectively by addressing cybersecurity issues from preventive, detective, and reactive perspectives, thereby forming a well-defined first line of cyberdefense. That **first line of cyberdefense** includes the establishment and implementation of access controls, a security operations center, security incident management processes, and vulnerability assessments and penetration tests. Those things are usually put in place and managed by a team of people with cybersecurity technical backgrounds. In most cases, a cybersecurity operations team reports to the chief information officer, chief technology officer, or IT department.

A cybersecurity management team of people with backgrounds in business cybersecurity is required in order to provide the **second line of cyberdefense**. It monitors the effectiveness of the technical controls the operations team has implemented, and it makes sure the company satisfies regulatory requirements while managing cybersecurity risks.

The cybersecurity management team must be distinct from the team responsible for the aforementioned technical activities. In some cases, it’s better when the two functions do not share the same reporting chain. That’s because specifying that only one of them is to report to the chief information officer inculcates cybersecurity responsibility through a wider swath of top management and avoids potential conflicts of interest.

An enterprise risk management framework gives greater legal and regulatory protection, but it’s not a cure-all for the ever–expanding range of cyberthreats. Assessing the likelihood of cybersecurity risks is inherently difficult because available historical data on cybersecurity incidents is limited, because detected incidents represent only a small portion of those that actually occur, and because technical vulnerabilities are always on the increase. In general, it’s safe to assume the risk is about 20% greater than what can be observed.

FIGURE 1: CYBERSECURITY MANAGEMENT AND OPERATIONS WITHIN IT

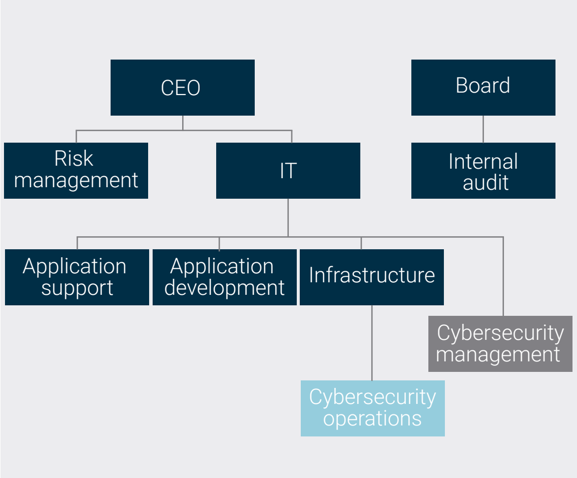


There are several models of cybersecurity risk governance plans that can reach throughout a business. Even though none are perfect, their differences reflect variations in company size, in the number of people involved, and in the cost of implementing a regime that follows the enterprise risk model.

Small and medium–size enterprises generally follow a model that makes no distinction between cybersecurity management and operations (figure 1). Although a commonly used model, it sometimes prevents a deep–rooted cybersecurity and risk management focus throughout the entire business.

Pro	Cons
Fewer resources required because it's only one team	Violates the segregation principle, meaning that cybersecurity is in the hands of the same people who must define, implement, and assess the organizational risk controls
Enables close management of cybersecurity risks related to IT assets	Top management lacks visibility on cybersecurity risks Makes it difficult to create a business case, limits internal investment, and eventually increases overall exposure to cybersecurity risks
	Lack of integration between cybersecurity risks and other enterprise risks
	Governance of cybersecurity risks limited to IT assets
	No enforcement authority or ability to collaborate with other business units

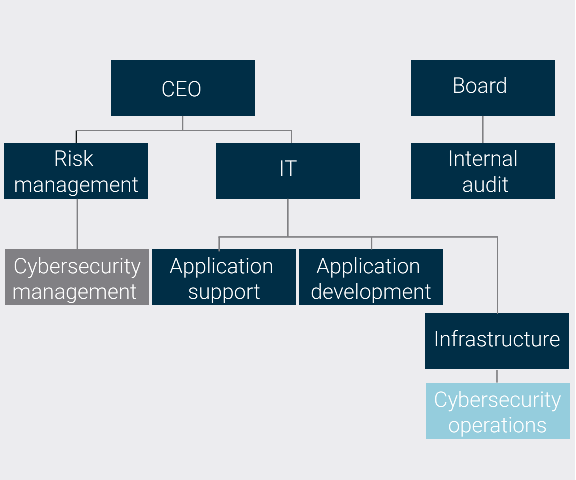
FIGURE 2: CYBERSECURITY MANAGEMENT SEGREGATED FROM OPERATIONS BUT WITHIN IT



In this scenario, the cybersecurity management team and the cybersecurity operations team are separate, but both of them report to the IT manager (figure 2). That structure can help with the technical aspects of risk management, but it might not give top management enough visibility about cybersecurity risks — and those cybersecurity risks may not be considered in alignment with other business risks.

Pro	Cons
Keeps governance and operations separate, enabling more-effective management of cybersecurity risks	No board and top management awareness of cybersecurity risks, limits internal investment, and eventually increases overall risk exposure
Good management of cybersecurity risks related to IT assets	Lack of integration between cybersecurity risks and other enterprise risks
	Governance of cybersecurity risks limited to IT assets
	Limited authority to enforce risk protocols or to collaborate with other business units

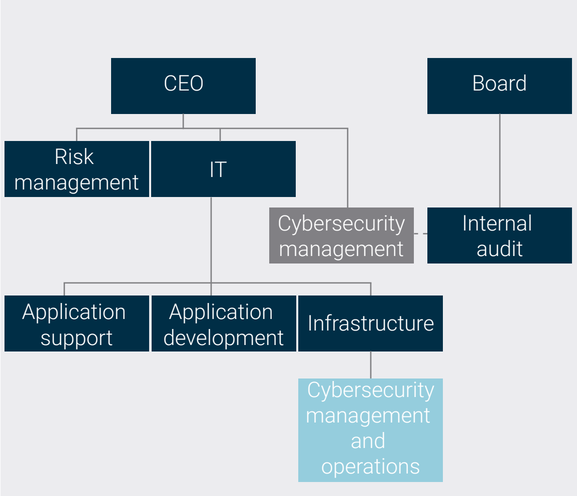
FIGURE 3: CYBERSECURITY MANAGEMENT WITHIN RISK MANAGEMENT



In this scenario, the cybersecurity management team and the cybersecurity operations team are completely segregated — both operationally and in their reporting chains (figure 3). Most likely, cybersecurity risks have been integrated into the overall enterprise risk management framework. In some cases, the cybersecurity management team will be installed within risk management.

Pro	Cons
Separate governance and operations enables more-effective management of cybersecurity risks	Limited board and top management awareness of cybersecurity risks
Balanced management of cybersecurity risks between IT and non-IT assets	Limited authority to enforce risk protocols or to collaborate with other business units
Integrates cybersecurity risks and other enterprise risks	

FIGURE 4: CYBERSECURITY MANAGEMENT AND OPERATIONS WITHIN IT



Organizing the governance of cybersecurity risks would likely require variations on these frameworks to suit individual companies. In that same vein, following are guidelines for defining a medium–term cybersecurity road map with the appropriate budget. A company must prepare a list of initiatives that explain how to reduce risk within the risk appetite limits defined by the enterprise risk management framework. Here are some essential steps to follow:

- **Define and quantify the required investment.** This is the money required to buy hardware, software, or services needed. It may be divided into operating expenses and capital expenditures.
- **Determine the level of effort required.** This is the number of man-hours required of internal employees to implement the plan. The number might be divided between the cybersecurity operations team, IT personnel, business lines, and, eventually, external service providers.
- **Describe the desired risk reduction.** This is a description of the intended extent of risk reduction.
- **Set the elapsed time for accomplishment.** This is the amount of high-level-management time required to deliver the initiative.

In this scenario, the cybersecurity governance team reports directly to the CEO, with a dotted line reporting to internal audit (figure 4).

Pro	Cons
Top management fully aware of cybersecurity risks	Lack of integration between cybersecurity risks and other enterprise risks
Separate governance and operations enable more-effective management of cybersecurity risks	
Balanced management of cybersecurity risks between IT and non-IT assets	
Authority to enforce risk protocols or to collaborate with other business units	

A cost–benefit analysis, performed possibly by using a data visualization tool, can demonstrate the cost of each part of the initiative and compare it with its projected benefits. The analysis can lead to a two- or three-year plan that stands as a robust cybersecurity road map for the entire organization. Don't be surprised to discover that the initiatives with the best cost–benefit ratio come from the ***people*** category, because the human factor is typically the weakest link in the cybersecurity chain.

MONITORING IMPLEMENTATION OF THE ROAD MAP

Finally, and most important, monitor the implementation of the framework according to the established road map. This can be supported by a business's internal audit function for achieving consistency and maximum effectiveness. Perform annual risk assessment exercises, and periodically reevaluate the company's current risk posture. Cybersecurity risks are always evolving, external threats are always broadening, and a business's vulnerabilities are always changing. But with top management and board involvement as an integral part of the risk management process, companies that apply international enterprise risk management standards to cybersecurity risks acquire a coherent and comprehensive organizational defensive posture for navigating the rapidly evolving, connected business climate. **A**

CONTACT THE AUTHORS:

Paolo Borghesi and Jon Rigby.

FOR MORE INFORMATION, CONTACT:

Jon Rigby
Director
+44 20 7098 7414
jrigby@alixpartners.com

ABOUT US

In today's fast paced global market timing is everything. You want to protect, grow or transform your business. To meet these challenges we offer clients small teams of highly qualified experts with profound sector and operational insight. Our clients include corporate boards and management, law firms, investment banks, investors and others who appreciate the candor, dedication, and transformative expertise of our teams. We will ensure insight drives action at that exact moment that is critical for success. When it really matters. alixpartners.com

The opinions expressed are those of the author and do not necessarily reflect the views of AlixPartners, LLP, its affiliates, or any of its or their respective professionals or clients. This article regarding Cybersecurity and risk management: lead from the c-suite ("Article") was prepared by AlixPartners, LLP ("AlixPartners") for general information and distribution on a strictly confidential and non-reliance basis. No one in possession of this Article may rely on any portion of this Article. This Article may be based, in whole or in part, on projections or forecasts of future events. A forecast, by its nature, is speculative and includes estimates and assumptions which may prove to be wrong. Actual results may, and frequently do, differ from those projected or forecast. The information in this Article reflects conditions and our views as of this date, all of which are subject to change. We undertake no obligation to update or provide any revisions to the Article. This article is the property of AlixPartners, and neither the article nor any of its contents may be copied, used, or distributed to any third party without the prior written consent of AlixPartners.