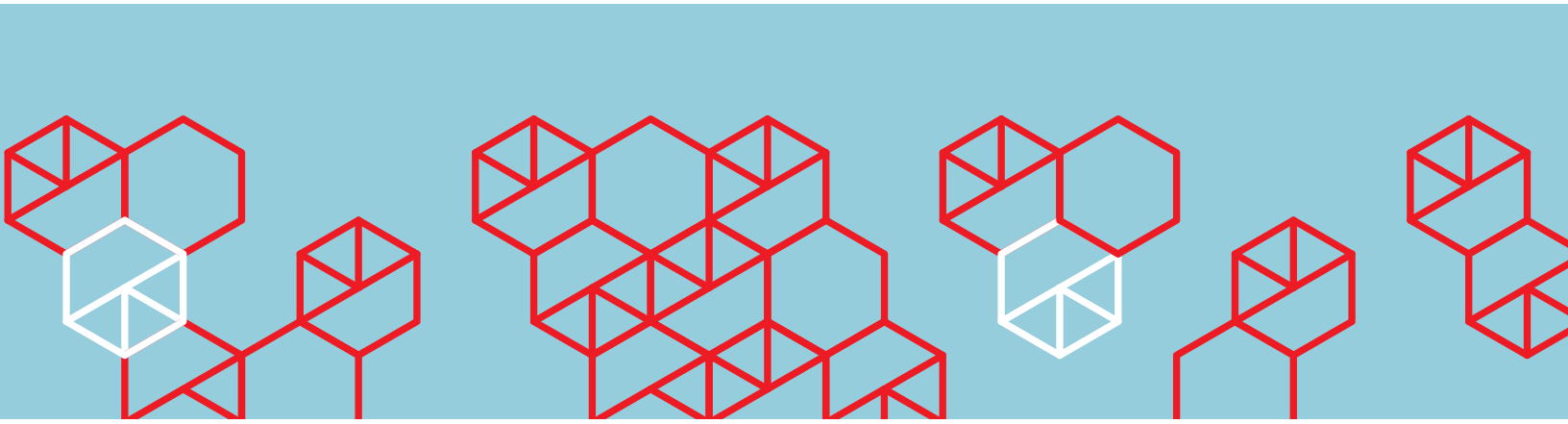
AlixPartners
when it really matters

DIGITAL

SEPTEMBER 2015

# Cybersecurity: building corporate resilience, encouraging protective transformation



Threats to governments' and businesses' cybersecurity could destroy $9 trillion to $21 trillion of potential global profit and value in the next five to seven years unless the public and private sectors handle them aggressively and effectively.[1]

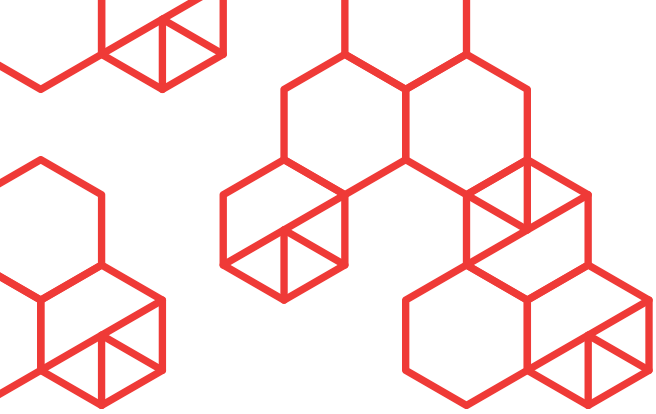
Boards attuned to their fiduciary responsibilities must understand and respond to the severity of both current and future risks to their businesses. Then they must invest in the security and governance of their information technology (IT) systems and operations.

Even though recent, chilling examples of data breaches have grabbed headlines and cost businesses billions of dollars, it is possible and certainly necessary to reduce exposure to such risk. Attackers, whether organised criminals or unaffiliated hackers think twice before targeting a company with good cybersecurity, focusing instead on less-well-protected alternatives.

Nonetheless, a cyberattacker needs to get *lucky only once*. Defenders must manage their internal and external business and system boundaries, constantly dealing with a host of threat vectors and actors—and still be *lucky all the time*. AlixPartners' experience shows companies must go beyond the requirements for basic technological protection in order to embrace genuine organisational transformation. The best approach is multidisciplinary, creating the most resilient cybersecurity and inculcating its importance from the c-suite to the shop floor.

Business interruptions, data privacy breaches, thefts of intellectual property, and damage to hard or soft assets all carry significant costs. A proxy theft of sensitive data during, say, a merger or acquisition

[1] National Association of Corporate Directors. *Cybersecurity—Director's Handbook Series*.



> For businesses with significant value in the areas of financial data, personal data, or intellectual property, advanced, persistent threats by organized crime have raised the stakes.

could fundamentally alter the outcome of the deal. A recent demonstration, in which a Jeep Cherokee was hijacked via the Internet, resulted in the recall of 1.4 million Fiat Chrysler vehicles—at considerable expense.[2] And there are more high- profile examples of privacy breaches: some of them involved data and healthcare records;[3] in another, Target lost 110 million personal records;[4] and in another, J.P.Morgan (one of the most secure enterprises in the finance sector) lost 465,000 customer records.[5] The cost to Target alone was $110 million, even after $38 million was recovered in insurance claim payments. However, the ultimate risks may well be those of reputational damage and customer, market, consumer, or shareholder confidence, which affect share prices, profits, and cash flow. In the quarter following Target's attack, company profits fell by 40%.[6] The recent adverse publicity and blackmail that targeted Ashley Madison—a Web site that facilitates discreet extramarital affairs—prevented a market capitalisation of up to £135 million ($210 million).[7] The last example shows how cyberattackers can strategically manipulate the market, although they were probably not motivated by financial gain in this instance.

These very public, very costly examples are notable because they are still exceptions. And without sufficient attention, many more companies and organisations would make that unenviable roster. A few well-chosen controls, implemented consistently across an enterprise, reduce risk markedly. Effective firewalls can stop common threats at a defended network boundary, but in the constantly shifting realm of cyberattack and defense, no IT system is fully secure; and in today's connected world, every industry sector has potential targets. Taking care of cybersecurity essentials is the first step, but the gap between the measures businesses perceive as adequate and what is actually effective still leaves many companies vulnerable.[8]

To add to the challenge, some of the most significant cybersecurity events have resulted from disenfranchised insiders' stealing data (Edward Snowden, who leaked massive amounts of information from the National Security Agency, is the obvious example) or unwary employees falling prey to a spear-phishing attack. For businesses with significant value in the areas of financial data, personal data, or intellectual property, advanced, persistent threats by organised crime have raised the stakes.

## A MULTIDISCIPLINARY APPROACH

Cybersecurity issues pervade every business sector and inform every risk/reward-balance decision a business makes. The digital age offers immense opportunity for business model transformation, as well as for increased efficiency, sustainable growth, and improved customer service. Cybersecurity remains pivotal not just to preserving a company's existing value but also to company growth.

2 *Financial Times,* July 25, 2015.
3 For example, involving Children's National Health System, which suffered unauthorised access to 18,000 individual e-mail accounts from July 26, 2014, to December 26, 2014.
4 Lee Munson, *ComputerWeekly.com*, March 14, 2014.
5 Reuters, December 6, 2013.
6 *New York Times,* February 26, 2014.
7 *LES,* July 21, 2015.
8 UK Government, *10 Steps to Cyber Security*.

An attacker doesn't recognise corporate, business, or even system boundaries but readily exploits any weaknesses that can be found. To strengthen an organisation's cybersecurity, a multidisciplinary contribution is essential if the business is to adequately confront its risk management responsibilities without slowing down operations, (even though typically, the most significant contributions come from technical expertise).[9] Therefore, the development of cybersecurity requires all means available to a firm to be integrated and deployed: leadership, operations, human resources, legal, communications, insurance, and technical. Workforce education is also a proven control, as is line management supervision. Human resources policies are required for screening employees with privileged access and for putting basic security rules in place. Weaknesses in partners' cybersecurity will affect the business and require careful commercial and contractual handling, and insurance can transfer some risk. Cybersecurity programs involve far more than IT projects. Given such complexity, the need for cultural change, and the realisation of benefits, cybersecurity programs require a transformational approach.

## THE BOARD AND ITS IT RESPONSIBILITIES

In the digital age, technology is the key business enabler and the engine of growth, which means it must be safeguarded from the very top of a company. CEOs, boards, and shareholders are increasingly focusing on cybersecurity. Some may join their chief information officers and chief information security officers in losing sleep over it—and they should. Still, cybersecurity resources cannot be limitless, nor can risk be reduced to zero. Boards must determine the necessary and acceptable cost of delivering cybersecurity while remaining competitive.

They must develop and communicate a cybersecurity narrative, a plan, and a mitigation program that are consistent with the needs of the business and the expectations of stakeholders— particularly, shareholders. That kind of complexity means that governance must be configured to handle the "wickedness" of the challenge.[10] It remains vital to maintain effective balance and excellent communication between the strategic corporate headquarters and the technical, dynamic expertise of the cybersecurity specialists.

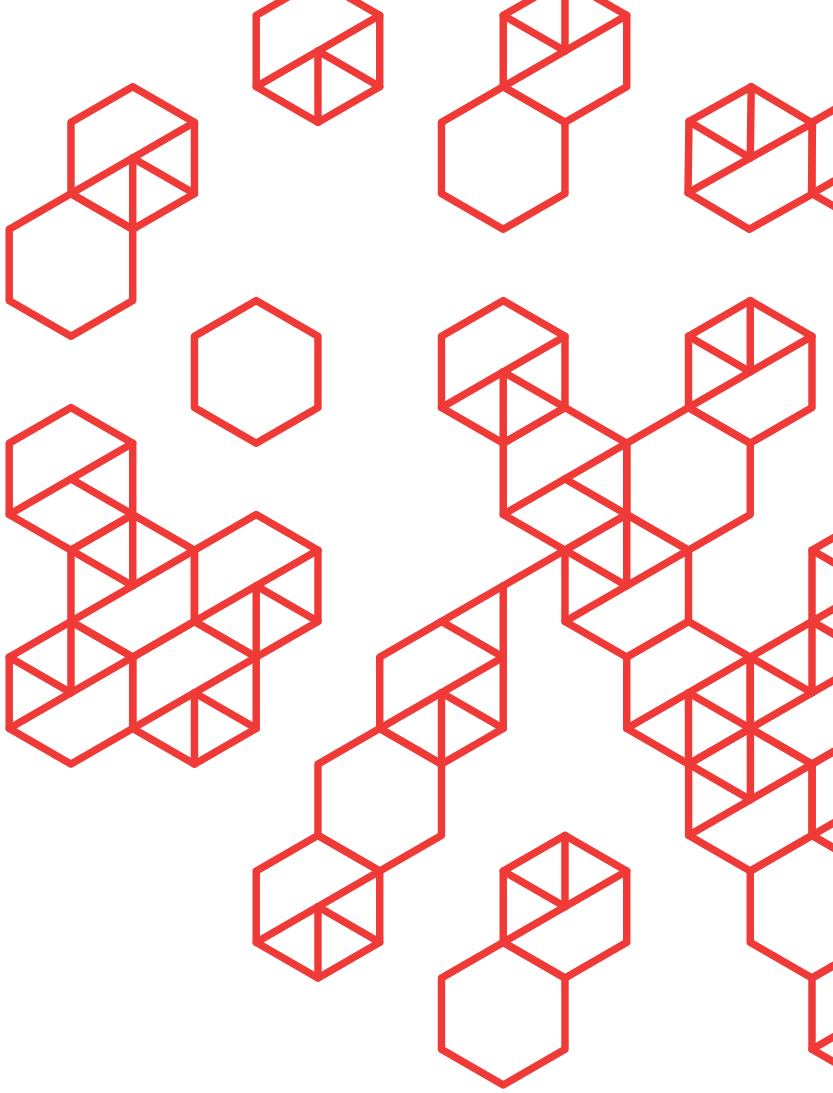
Most companies will have information security risks on their register, but too often, the description of these risks is either overly generic or excessively technical. A more nuanced and multidisciplinary approach is required. Only the board can assess which information assets or business processes are critical (because it is those that are under attack) and how much their loss or interruption would cost. Predicting a company's risk exposure in advance of the disruption it seeks to avoid and then quantifying it are difficult endeavours. Ultimately, cyber is a contested domain and the most accurate data is either commercially or nationally sensitive. Despite improved sharing and better communications, situational awareness and knowledge will always be incomplete and these gaps effectively create opportunities for cybercrime.

## PREPARING FOR THE PROBABLE

Cybercrime is a low-risk activity for the perpetrator, and if the potential gains exceed the time and cost invested, the purveyors of advanced, persistent threats are all but unstoppable. The state use or endorsement of proxy agents (deploying these top-end capabilities) has blurred the line between state and non-state cyberattack[11]; fundamentally increasing the challenge faced by the private sector and the preservation of a secure, global, digital environment in which to conduct business. A cyberattack should register as a high-impact risk—and a likely one—for any corporate board. When a company suffers a cybersecurity event, leadership must respond rapidly and openly to preserve the company's reputation and value. Leadership can expect to be held accountable for the impact and subsequent handling of the event. A report on any data breach or other event almost always exceeds the value of any losses involved. A company must be able to communicate—and demonstrate—that it has taken reasonable cybersecurity precautions, that loss or damage was stopped early, and that the company has the resources to remediate losses in good time.

The imperative is to learn those skills and develop a cyber contingency plan well in advance of the maelstrom of an event and subsequent reduction in corporate value. **A**

[9] Luke Forsyth, "So secure it's unusable," LinkedIn Pulse, May 5, 2015; https://www.linkedin.com/pulse/so-secure-its-unusable-luke-forsyth?trk=prof-post.
[10] C. West Churchman. "Wicked Problems." *Management Science* 14(4)(December 1967), B141-B142
[11] FT Online Marauders dated 5 Sep 2015




## 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