Executive Insights

Volume XVIII, Issue 45

Beyond Technology: Developing a Holistic Approach to Cybersecurity

Cybersecurity is a key concern today for businesses around the globe. Recent reports that hackers stole 500 million passwords and usernames from Yahoo represent the latest in a catalog of high-profile attacks, proving that even the largest and most well-resourced businesses are not immune to the attentions of cybercriminals.

The global economic cost of cybercrime was $445 billion in 2014, according to a Center for Strategic and International Studies report sponsored by McAfee. Perhaps most worrying, criminal capability appears to be outpacing governments' efforts to respond, and the World Economic Forum has warned that cyberattacks could cause global economic losses of up to $3,000 billion over the next six years.

With risks so high, there is no shortage of advice on cybersecurity. However, most focus is on IT risk identification and technology-oriented solutions, with too little attention paid to the broader, strategic causes and implications.

L.E.K. Consulting recommends a holistic approach to cybersecurity that addresses both the technology and people-based risks, and also accounts for the strategic, commercial and operational impact of controls, taking into account the trade-off between risk reduction and competitive advantage.

We have identified four key areas that companies often overlook when developing their approach:

1. Focus on people, not just technology
2. Beware of hidden costs
3. Rethink the cyber business model
4. Plan for failure

1. Focus on people, not just technology

Too often, vulnerable companies and cyber service providers think about technology, IT and tools as being both the source of and the answer to problems. A key element that is not sufficiently examined is the role of people, both inside and outside the organization.

Globally, 95% of all cybersecurity incidents involve some degree of human error, according to IBM. In the U.K., 50% of companies say their most significant breach was caused by human error,[1] with accidental actions carried out by staff or contractors cited as the largest single source of breaches, far larger than criminal activity (see Figure 1).

Similarly, in the U.S., half of the Small Business Administration's top 10 tips for cybersecurity relate to people and staff.

[1] 2015 Information Security Breaches Survey, U.K. Government

Beyond Technology: Developing a Holistic Approach to Cybersecurity was written by **Clare Chatfield** and **Larry Verge**, partners at L.E.K. Consulting. Clare is based in Paris and Larry is based in London.

For more information, please contact **strategy@lek.com**

L.E.K. INSIGHTS@WORK

Figure 1
What was the origin (threat actor / source) of the breach?
Based on 39 responses

However, if people are part of the cybersecurity problem, they are also critical to the solution. Companies need to consider a range of measures, from better communication, training and process modifications to compliance for employees across their organizations.

The costs of these aspects of cyber defense are often only a fraction of the outlay on technical solutions. For example, IBM estimates that employee training alone can save, on average, $8 per record breached, or 66% of the cost savings offered by the extensive use of encryption.

2. Beware of hidden costs

Technology advances in areas such as mobility, cloud and collaboration are providing valuable sources of efficiency and competitive advantage to companies. But this drive for easy and rapid data access opens up organizations to cyberattacks.

One example is the trend toward BYOD (or "bring your own device"), in which employees use personal technology such as smartphones and tablets to access business information, for example by reading company emails on the way to work. Nearly 70% of employees who own a smartphone or tablet use it to access corporate data.[2]

While convenient, BYOD carries security risks; not only is potentially confidential data being accessed in public locations, but the company has no control over the number of copies or the destination of the data.

Faced with such risks, the natural reaction for companies is to put up more impenetrable barriers to intruders and place heavy restrictions on how employees use technology.

This can create several problems.

First, blanket bans may well lead to additional cost for businesses; for example, organizations with pro-BYOD policies save an average of 17% a year on their communications bill, according to Samsung Electronics.

Second, IT barriers such as firewalls can lead to heavier and slower systems, create administrative burden, and work against the principles of speed and flexibility that represent a competitive edge in many industries and service sectors.

Third, when employees are faced with restrictions on their IT activities, many will respond by finding ways around the problem, which may create even more risks. Employees denied the opportunity to access emails or data from their own devices, for example, may copy information to USB sticks or personal email accounts to work on at home.

Cybersecurity risk needs to be examined from a holistic perspective in the company. There are real costs and other impacts associated with protection that is not designed with critical business needs in mind.

As a prerequisite to developing or reviewing their cybersecurity architecture, businesses should ask themselves what the economic trade-offs are in different approaches, and hence the optimum level and nature of protection.

We find that businesses frequently overlook a qualitative and quantitative analysis of the impact of cybersecurity issues and fail to complete a risk-reward analysis of the different options available.

3. Rethink the cyber business model

Companies today need to take a new approach to cybersecurity.

Given the high stakes involved, cyber protection should be treated as a top priority, discussed and planned at board level. In some industries and companies, this is already the case, driven in part by regulation. Today, however, only 40% of boards frequently ask about cyber readiness and only half of U.S. companies have an operational cyber response plan in place.[3]

[2] Ovum
[3] Global Economic Crime Survey 2016, PWC

An effective response to cyber risk needs to be integrated into the broader strategic plan for the business. L.E.K. believes that decisions must be based on cybersecurity's place as a fundamental part of company operations. Key questions include:

- How does the business's approach to data affect its cybersecurity risk?
- How would a security breach impact not only the business but its customers?
- What would a breach mean for the longer-term reputation and viability of the company?
- What steps should be taken to mitigate cybersecurity risks? What should the focus be, given key areas of risk (for example, reducing the amount of personal data on customers)?

As part of this strategic evaluation, companies also need to carefully consider what can be managed internally and what should be outsourced to specialists and expert providers. There is an often-held assumption that cybersecurity can and should only be handled in-house, but the risks are evolving so rapidly in both nature and scale that internal IT management and teams are not always skilled or resourced to respond effectively. External providers can offer a much-needed outsider's perspective that is also likely to prove cost-effective. External specialists need to be carefully evaluated, but outsourcing some cybersecurity aspects to managed service providers may well be safer and faster than trying to build internal expertise from scratch.

4. Plan for failure

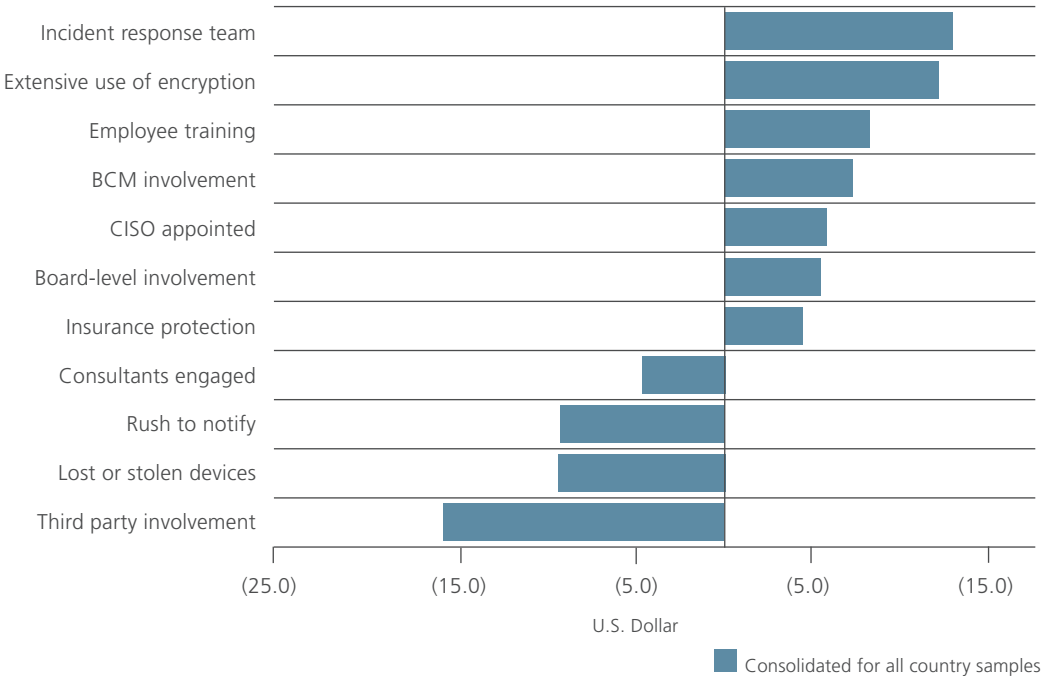
Even with extensive safeguards in place, the reality is that eliminating all cyber threats is impossible. An effective cybersecurity strategy means preparing for the worst. This can help limit damage in the event of a breach, and avoid a knee-jerk reaction that can be costly and inefficient.

Having an incident response team and business continuity management plan has been shown to reduce the cost of a data breach (see Figure 2) and best-practice companies work through contingency plans for a range of cyber risks (see Figure 2).

Some aspects may be relatively straightforward, such as IT disaster recovery, while others are best tackled with advice from specialists in areas such as public relations, forensic/IT security, data breach resolution, identity theft and credit monitoring.

One specialist area that is becoming increasingly important is cyber insurance coverage, which can hedge against the costs of a security breach (including incident response and investigation, third-party liabilities, public relations, business interruption and reputational damage).

Figure 2
Impact of 11 factors on the per capita cost of data breach
Consolidated view (n=350), measured in US$



Source: Ponemon Institute (Sponsored by IBM) 2015 Cost of Data Breach Study

Figure 3
Cybersecurity contingency planning

Contingency planning should include five main components:

1. Set up an organization-wide incident response team, with board approval / oversight.
2. Establish an incident response plan to cover wider impacts of a security incident. These include:
   - Legal obligations (e.g., notification of customers)
   - Reporting obligations (e.g., law enforcement, regulatory bodies)
   - Public relations plans (e.g., crisis communications, notification of investors and business partners, media coverage)
   - Customer communication and care
   - Establishing agreements with third-party suppliers (e.g., legal counsel, crisis communications)
3. Maintain user awareness regarding reporting a breach.
4. Regularly test / rehearse incident management plans.
5. Incorporate lessons learned from previous security breaches.

Conclusion

Cybersecurity risks are increasing and are constantly evolving in nature. The likelihood is that all organizations will face a breach at some point, whether intentional or accidental.

A strategic and value-based approach to managing the risks involves developing a plan that can evolve along with the risks and the company's priorities, addressing both human and technology factors.

At L.E.K. we have found that the application of sound cost/benefit analyses, make-or-buy assessments, and risk identification and mitigation techniques are as applicable to cybersecurity as they are to any business strategy development.

About the Authors

Clare Chatfield is a senior partner at L.E.K. Consulting. She is the head of L.E.K.'s Paris office and a member of L.E.K.'s European Regional Management Committee. Clare has more than 25 years of experience working for a broad range of international corporate clients across multiple industries, including technology infrastructure and IT services. Clare also leads L.E.K.'s Energy & Environment practice.

Larry Verge is a senior partner in L.E.K.'s European Strategy practice and a member of L.E.K.'s Global Leadership Team. He has more than 30 years of experience providing advice to a wide range of clients. Larry has worked across a number of different sectors, focusing on technology applied to a range of consumer and industry sectors. His work has covered strategy development for some of the firm's largest clients, as well as a wide range of mergers and acquisitions projects.

About L.E.K. Consulting

L.E.K. Consulting is a global management consulting firm that uses deep industry expertise and rigorous analysis to help business leaders achieve practical results with real impact. We are uncompromising in our approach to helping clients consistently make better decisions, deliver improved business performance and create greater shareholder returns. The firm advises and supports global companies that are leaders in their industries — including the largest private and public sector organizations, private equity firms and emerging entrepreneurial businesses. Founded more than 30 years ago, L.E.K. employs more than 1,200 professionals across the Americas, Asia-Pacific and Europe. For more information, go to www.lek.com.

L.E.K. INSIGHTS@WORK