Why cybersecurity is a strategic issue

Is your business one hack away from disaster?

By Syed Ali, Vishy Padmanabhan and Jim Dixon

BAIN & COMPANY

Syed Ali is a principal with Bain & Company in Chicago. Vishy Padmanabhan is a partner with Bain & Company in Dallas. Jim Dixon is a partner in Bain's Palo Alto office. All three work with Bain's Global Information Technology practice.

When you think of the billions of dollars organizations spend to protect their digital assets, it's amazing that hardly a week goes by without news of a major security breach. We see not only more attacks, but larger, more complex and targeted incursions on organizations for financial gain (see Figure 1). Some enterprises face advanced persistent threats (APTs), a highly sophisticated form of malware that permeates the organization, mutates into variants, remains innocuous and undetected for a long time, and stealthily accesses and transmits corporate assets. The sought-after digital assets include intellectual property (IP), trade secrets, and customer and financial data (see Figure 2).

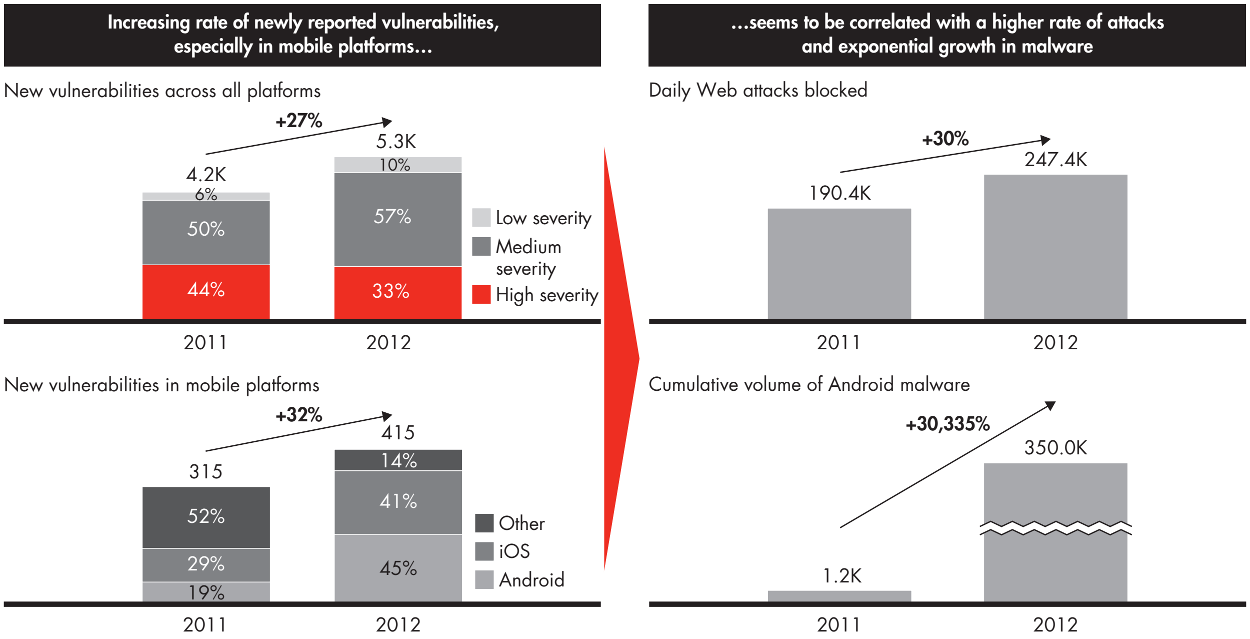
Organizations are having a tougher time mitigating security breaches, and the average financial impact of each breach on an organization is increasing (see Figure 3). What's more, it's becoming harder to keep these attacks out of the news. Often, clients or regulatory agencies require companies to disclose breaches; in other cases, attackers themselves distribute the pilfered information online. In many cases, the consequences for organizations can be devastating in terms of lost revenue, impugned reputations and financial repercussions.

For example, an October 2013 attack on Adobe resulted in the theft of customer data from 38 million accounts and of valuable source code behind some of Adobe's most widely used products, including Reader, PhotoShop and ColdFusion.

Only two months later, in December 2013, Target Corporation confirmed that it suffered a massive security breach resulting in the loss of credit and debit card data on 40 million customers over a 19-day period. The data may have been harvested by malware affecting physical point-of-sale systems at nearly 2,000 Target stores.

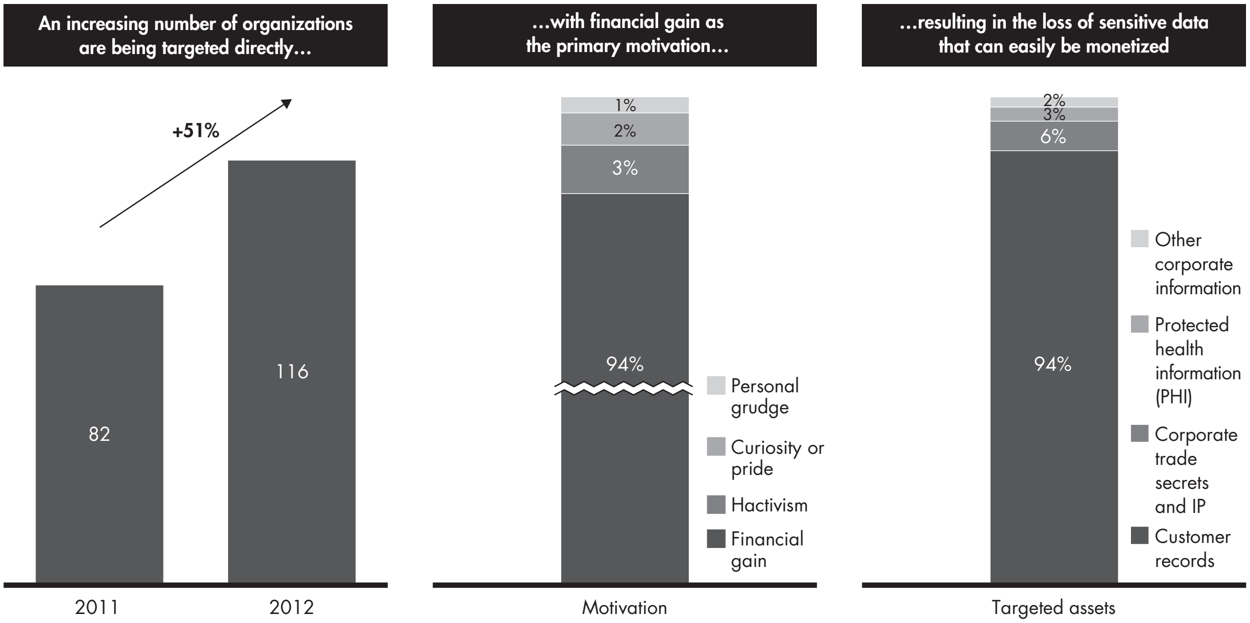
The immediate consequences for a company dealing with a customer data breach are severe and may include negative press, sales and stock price decline (at least immediately after the breach), the threat of lawsuits from customers and partners, and long legal investigations. When attackers gain access to the source code

Figure 1: Deeper and broader security vulnerabilities seem to correlate with more attacks and malware



Sources: MITRE CVE; Symantec; Trend Micro; Bain analysis

Figure 2: Most attacks come from outsiders looking for financial gain



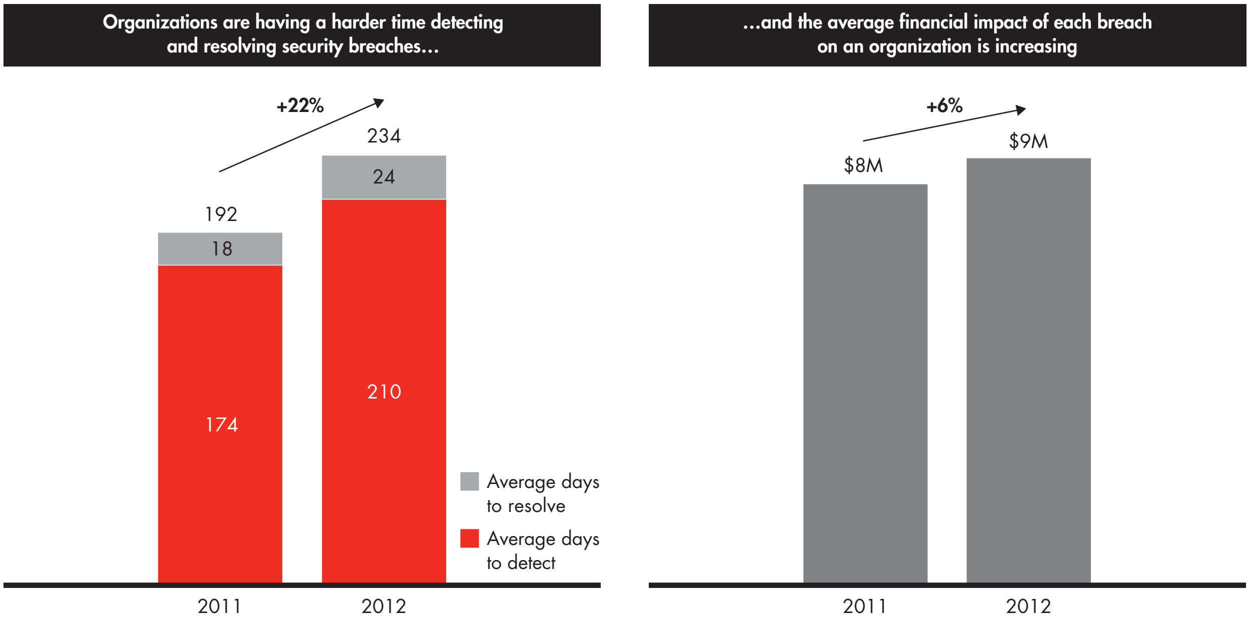
An increasing number of organizations are being targeted directly…

…with financial gain as the primary motivation…

…resulting in the loss of sensitive data that can easily be monetized

Sources: Symantec; Verizon 2011 investigations; Trustwave; Bain analysis

Figure 3: Security breaches are becoming more difficult and expensive to detect and mitigate



Organizations are having a harder time detecting and resolving security breaches…

…and the average financial impact of each breach on an organization is increasing

Sources: Trustwave; Ponemon Institute; Bain analysis of software products, they can find and exploit new vulnerabilities (so-called zero-day attacks) that could affect corporate and customer systems, data and devices.

With stakes so high, CEOs and boards must begin to think about security in a new way. IT security—a task that could once be delegated to the IT staff—has become a top-level strategic issue because the consequences of failure can ruin a business. Any organization may be only a few hacks away from disaster.

And yet, every organization that found itself on the wrong end of a security breach already had some form of cybersecurity in place. The names in recent headlines include banks, technology and media companies, retailers, research universities as well as security agencies—none of which are new to the game of protecting information. So how is it that they found themselves ill-equipped to deal with the rising tide of threats?

In our experience working with many leading enterprises on this important and sensitive issue, we see too many organizations that fail to align their IT security capabilities with their larger goals and appetite for risk. At some companies, business and IT don't discuss emerging threats or the relative importance of different classes of digital assets. Not surprisingly, we frequently see disconnects between an organization's risk-management efforts and the development of necessary cybersecurity capabilities. And too often, we see fits and starts, as teams take an inconsistent approach to security planning, operations and funding. Taken together, these mistakes create gaps in strategy and operations that leave the organization vulnerable.

New challenges for cybersecurity

Cybersecurity has never been more essential, for at least four major reasons. First, companies have more digital assets than they did 10 years ago, and these assets are worth more than they were before. They include customers' personal, financial and transaction information; proprietary assets, including source code for products; automated business processes; sensitive communications with suppliers and partners; and other data. The security around these assets varies greatly depending upon the perceived (as opposed to the actual) financial and strategic value to the business, as well as the effectiveness of the security technologies and processes in place.

What's more, organizations are shifting to hybrid cloud architectures as they continue to adopt software, security and other solutions as services (SaaS, SECaaS and so on). Historically, digital assets were protected within the company's data center, where it was easier to guard the perimeter and manage user access, authorization and authentication from known locations and devices. Today, corporate and customer data resides in the organization's own data centers as well as public and private clouds, distributed across remote locations. While hybrid cloud architectures offer significant economic benefits, their adoption requires a more sophisticated approach to cybersecurity, including security management at the level of individual digital assets and integrated monitoring and management capabilities across the hybrid cloud environment.

Further complicating the challenge is the pervasive use of mobile devices by staff and executives. Corporate IT now has to manage the security of many more platforms and devices, some owned by the company and others that belong to employees who use them under bring-your-own-device (BYOD) plans. A recent survey by ISACA[1] found that up to 66% of organizations will soon adopt BYOD policies, yet half of IT staff members remain concerned about the inherent security risks. To manage these policies effectively, IT organizations will need to provide ubiquitous security across many devices and comprehensively manage user identity and access to sensitive corporate data.

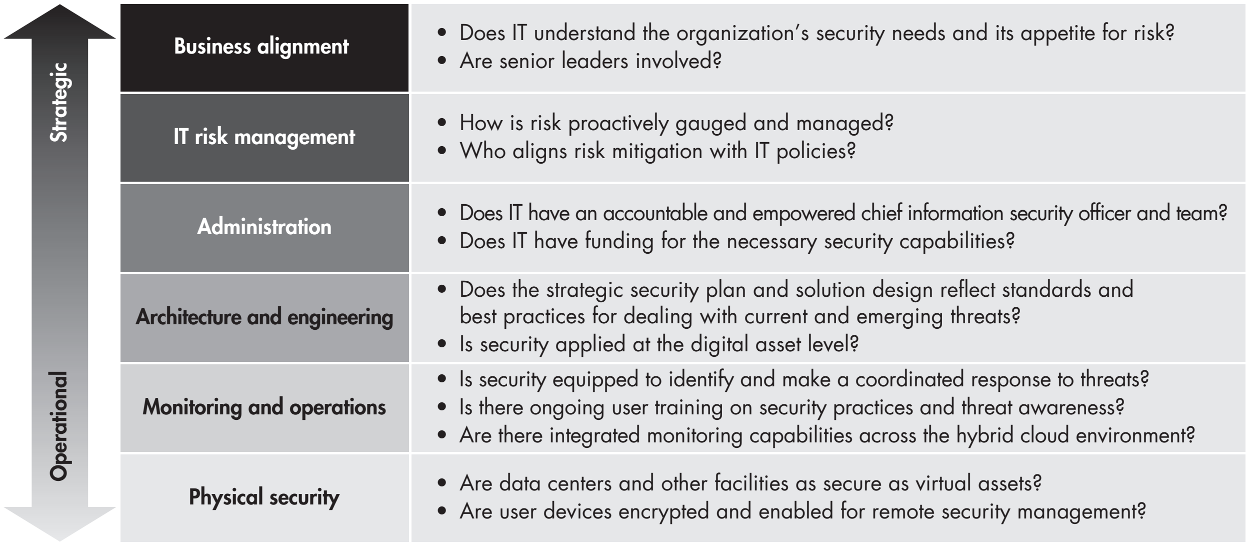
Finally, compliance remains the most important cybersecurity driver, especially for companies in regulated industries or with contractual obligations. In a recent Bain survey, more than 75% of CIOs identified compliance requirements as the main determinant of investment in IT security. Another recent survey of IT staff by ISACA found that outside of compliance obligations, IT has insufficient resources and limited business engagement for effective risk management.[2] These findings highlight the operational approach to cybersecurity taken by many organizations. Compliance should define the lower bound for security capabilities while the upper bound should aspire to meet the organization's strategic priorities, including IP protection, continuous operations and a secure corporate reputation.

Protecting your data, reputation and business

Leading organizations take a more strategic rather than an operational approach to security to respond to the new challenges.

- **Understand the organization's key assets and appetite for risk.** Align business and IT leaders on the prioritization of digital assets based on value and risk to the organization to ensure the proper design of technology, processes and supporting resources. For example, customer data, point-of-sale and order management systems are a higher priority while marketing and promotion systems may be lower.
- **Identify the security risks and gaps.** Assess current security capabilities and determine the likelihood of experiencing known and emerging risks. Business and IT leaders should then align on the gaps and the estimated mitigation costs.
- **Define the cybersecurity strategy.** Based on a thorough understanding of the organization's security priorities and gaps, IT should create comprehensive technology, process and organizational designs and blueprints with strategic and operational elements that protect digital assets *(see Figure 4)*.
- **Emphasize gaps, priorities and strategy to the CEO and board.** Leadership should know about the security-related risks and gaps they face, so they can understand the importance of the investments required.
- **Engage recognized security specialists.** As the threat landscape expands and attacks become more sophisticated, organizations should work closely with firms that can provide ongoing services to diagnose, redesign and monitor their cybersecurity.

Figure 4: Bain's approach to cybersecurity aligns strategic imperatives with the necessary operational capabilities



Business alignment	• Does IT understand the organization's security needs and its appetite for risk? • Are senior leaders involved?
IT risk management	• How is risk proactively gauged and managed? • Who aligns risk mitigation with IT policies?
Administration	• Does IT have an accountable and empowered chief information security officer and team? • Does IT have funding for the necessary security capabilities?
Architecture and engineering	• Does the strategic security plan and solution design reflect standards and best practices for dealing with current and emerging threats? • Is security applied at the digital asset level?
Monitoring and operations	• Is security equipped to identify and make a coordinated response to threats? • Is there ongoing user training on security practices and threat awareness? • Are there integrated monitoring capabilities across the hybrid cloud environment?
Physical security	• Are data centers and other facilities as secure as virtual assets? • Are user devices encrypted and enabled for remote security management?

Source: Bain & Company

[1] ISACA: 2013 IT Risk/Reward Barometer – Global Results

[2] ISACA: 2012 Study on Application Security

Shared Ambition, True Results

Bain & Company is the management consulting firm that the world's business leaders come to when they want results.

Bain advises clients on strategy, operations, technology, organization, private equity and mergers and acquisitions. We develop practical, customized insights that clients act on and transfer skills that make change stick. Founded in 1973, Bain has 50 offices in 32 countries, and our deep expertise and client roster cross every industry and economic sector. Our clients have outperformed the stock market 4 to 1.

What sets us apart

We believe a consulting firm should be more than an adviser. So we put ourselves in our clients' shoes, selling outcomes, not projects. We align our incentives with our clients' by linking our fees to their results and collaborate to unlock the full potential of their business. Our Results Delivery® process builds our clients' capabilities, and our True North values mean we do the right thing for our clients, people and communities—always.

Key contacts in Bain's Global Information Technology practice:

Americas:

Syed Ali in Chicago *(syed.ali@bain.com)*
Steve Berez in Boston *(steve.berez@bain.com)*
Vishy Padmanabhan in Dallas *(vishy.padmanabhan@bain.com)*
Rudy Puryear in Chicago *(rudy.puryear@bain.com)*
Jean-Claude Ramirez in São Paulo *(jean-claude.ramirez@bain.com)*
Jonathan Stern in San Francisco *(jonathan.stern@bain.com)*
Rasmus Wegener in Atlanta *(rasmus.wegener@bain.com)*

Asia-Pacific:

Arpan Sheth in Mumbai *(arpan.sheth@bain.com)*
Peter Stumbles in Sydney *(peter.stumbles@bain.com)*

Europe, Middle East and Africa:

Thomas Gumsheimer in Frankfurt *(thomas.gumsheimer@bain.com)*
Marc Lino in Amsterdam *(marc.lino@bain.com)*
Stephen Phillips in London *(stephen.phillips@bain.com)*
Sachin Shah in London *(sachin.shah@bain.com)*

For more information, visit **www.bain.com**

Amsterdam • Atlanta • Bangkok • Beijing • Boston • Brussels • Buenos Aires • Chicago • Copenhagen • Dallas • Dubai • Düsseldorf • Frankfurt
Helsinki • Hong Kong • Houston • Istanbul • Jakarta • Johannesburg • Kuala Lumpur • Kyiv • London • Los Angeles • Madrid • Melbourne
Mexico City • Milan • Moscow • Mumbai • Munich • New Delhi • New York • Oslo • Palo Alto • Paris • Perth • Rio de Janeiro • Rome • San Francisco
São Paulo • Seoul • Shanghai • Singapore • Stockholm • Sydney • Tokyo • Toronto • Warsaw • Washington, D.C. • Zurich