Executive Series

Security Essentials for CIOs

Securing the extended enterprise

Highlights:

Diverse and proliferating data relationships are a source of growing security concern. The challenge is to implement policies and best practices governing your data, no matter where it goes. Enterprises must take vigorous steps to keep their entire information ecosystem secure including vendors, suppliers, contractors, acquisitions and partners.

Let's assume that your security operations are stellar. You have procedures in place to keep software patches up to date, and a team that responds to incidents within minutes. A relentless focus on security permeates your enterprise. In short, in-house you're doing everything right. But how about outside your organization? Chances are a contract company is handling payroll, or perhaps employee retirement plans. Is your data safe with them?

Risk in the traditional supply-chain is no secret. A flood in Asia or a strike in Brazil can knock out crucial components and paralyze distant manufacturers. But an enterprise's far-flung data relationships are also a source of growing security concerns—and these are expanding dramatically. As organizations coordinate manufacturing, distribution or marketing, they share data with each other—and, potentially, with a host of thieves, spies and other bad actors. Indeed, whether operating supply chains or hiring service providers, enterprises are rapidly creating potential new vulnerabilities outside their own firewalls.

Just as firms must police suppliers, contractors and vendors for poor workmanship or unfair labor practices, they must also take vigorous steps to keep their entire information ecosystem secure. Credit card companies found this out the hard way earlier this year with a high-profile breach at a card transaction processing company.[1] This problem isn't going to go away. PwC's 2012 Global State of Information Security Survey sees it as a growing problem, with increasing numbers of respondents identifying partners and suppliers as a source of breaches (up from 8% to 15% between 2009 and 2011).[2]

The risks in an information ecosystem can appear daunting. Legions of new players around the world dip into different levels of your data, whether for years on end or just a day or two. Some users may require access to privileged and sensitive information, such as employee social security numbers or health records. Others may just need to provide basic back office services. The challenge is to implement a series of policies and best practices governing your data, no matter where it goes.

We are constantly managing these challenges at IBM, and we have come up with a set of tips for advancing security for the extended enterprise:

1. Build security into every relationship—from the very start. The only way to establish control is to design it from the beginning into every relationship. This means establishing clear security norms and procedures for every entity entering into a relationship where data is exchanged. Organizations should work with their partners, contractors, suppliers and vendors to be aware of how their data will be handled and the measures that will be used to protect the information.

2. Watch the clouds. Increasingly, enterprises are outsourcing data management to cloud computing centers. This is especially prevalent among those offering software as a service (SaaS). This means you have to extend your security focus to your partners' suppliers. They must convince you that they're operating securely and complying with laws covering your data, both at home and in the data center's jurisdiction. And your supplier should not be free to move to another cloud provider without an explicit agreement from you.

3. Focus on the small fry, too. It's natural to focus on hefty partners, the banks or insurance companies that handle petabytes of sensitive data. And they should be vetted thoroughly. But many of these big firms have had to comply with tight industry regulations for years. Some of the risks come from smaller start-ups, who might have contracts for portal apps or marketing campaigns. Many of these companies are born around an idea or a single service and they may not focus their limited resources on security. What's more, they're much more likely to run their apps in clouds, which may raise further concerns. These companies still have to follow basic security requirements, even if they have limited resources to do so.

Extending the security perimeter

- **Build** security into every relationship—from the start.
- **Develop** tight procedures for M&A—from due diligence through integration
- **Extend** your focus to your partner's suppliers—both large and small
- **Assume** that nothing is ever settled

Figure 1

4. Develop tight procedures for M&A. Vulnerability can skyrocket during mergers and acquisitions. As soon as news of a pending acquisition is announced and goes viral on Twitter, target companies can experience a blizzard of probes and attacks from hackers and thieves. For these attackers, M&A provides rich opportunity, a chance to insinuate themselves or their malware into the acquiring company by penetrating the defenses of its new prize.

Security procedures during M&A consists of three steps. The first is due diligence. Does the target company come with a legacy of previous breaches and attacks? If so, it could raise questions about the viability of the acquisition, or at the very least spur a comprehensive effort to address vulnerabilities. The second step is to mount a defense for attacks that could

follow the announcement. Companies should work closely with acquisitions, as soon as the law permits, to fortify their defenses. The third step is an extended effort to beef up security, with software, education and best practices, so that when the target firm merges its network—six months or even a year later—it is every bit as secure as the acquiring company.

The number of respondents identifying partners and suppliers as sources of breach has increased from

8% to 15%

between 2009 and 2011.[2]

Source: PwC

5. Assume that nothing is settled—ever. Change in security is relentless. A breach in one supplier can require a cascade of fixes and adjustments across the supply chain. New data laws around the globe can lead to new compliance requirements. If you don't watch it, your data in a country may fully comply with the law one day, and not the next.

Security issues, like the streams of data underlying every aspect of business today, continue to increase. To keep up, every organization requires the efforts of a top-notch security team, one monitoring the entire extended enterprise. It's loads of work, and the job is relentless. But staying on top of your data, wherever it may go, is the price of doing business in the hyper-connected world.

Join the conversation

To read additional articles, learn more about Security Essentials for CIOs, or share your thoughts with other security leaders join us at ibm.com/smarter/cai/security.

About the author

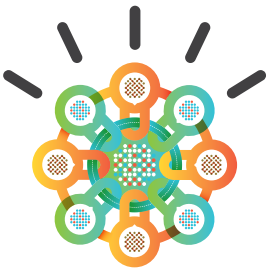
Kristin Lovejoy is Vice President of IT Risk, Office of the CIO, IBM. She can be contacted at klovejoy@us.ibm.com.

About IBM Center for Applied Insights

The IBM Center for Applied Insights (ibm.com/smarter/cai/value) introduces new ways of thinking, working and leading. Through evidence-based research, the Center arms leaders with pragmatic guidance and the case for change.

[1] "Global Payments Data Breach Exposes Card Payments Vulnerability", Forbes, April 3rd, 2012, http://www.forbes.com/sites/greatspeculations/2012/04/03/global-payments-data-breach-exposes-card-payments-vulnerability/

[2] "Eye of the storm—Key findings from the 2012 Global State of Information Security Survey", PwC, http://www.pwc.com/jg/en/media-article/2012-global-state-of-information-security-survey.jhtml



IBM Global Services
Route 100
Somers, NY 10589
U.S.A.

Produced in the United States of America
September 2012

WGW03015USEN-01