FT .com
FINANCIAL TIMES

Published March 22, 2013

Striking a Balance Between Extracting Value and Exposing Your Data to the Bad Guys

By Eric Openshaw and Irfan Saif

Financial Times Connected Business Section
http://www.ft.com/intl/cms/s/0/35993dce-933a-11e2-9593-00144feabdc0.html#axzz2OYaUSn3D

Headlines you may soon read: “State-sponsored attack breaches 20 major US software vendors; Source code and product roadmaps stolen” and “Claims processing firm accidentally releases over 200m social security numbers with medical history, mother’s maiden name, other personal information.”

Together with real news stories in recent months, these hypothetical headlines reflect the growing sophistication and intensity of cyber-attacks as well as the general public’s growing awareness of their vulnerability to security breaches and other forms of attack.

Catastrophic security breaches are feared to be imminent. The looming impacts range from stolen intellectual property and the inability to conduct business, to significant brand erosion and lost competitive advantage. The message for executives trying to make sense of what it means to company IP, data and operations is that the game has changed and it’s time for leadership and attention from the top.

Information security is an enterprise-wide concern that reaches well-beyond the IT department as companies increasingly depend on business and operating models that require data to be shared but also protected. As the landscape of threats keeps changing, companies have to balance the risks of lost or compromised data against the risks of restricting information flow or losing competitiveness.

Negotiating the tension between these two demands, while also striking the appropriate balance of prevention, detection, response and corrective mitigation and improvement, requires real ownership and top-down direction.

Consider the ‘Partnering for Cyber Resilience’ initiative, signed by more than 70 private-sector executives and government leaders at the World Economic Forum in Davos in January 2013, which signaled the increased awareness of cyber risk and data security in the ‘C’-suite and the boardroom.

While the initiative focused on a more coordinated response to threats, including the possibility of a Center for Disease Control-type global clearinghouse, it should also help elevate data security as a primary business issue, requiring better alternatives and resources commensurate with the risk to the company’s financial health and competitive position.

In fact, 75 per cent of respondents in a recent Deloitte Touche Tohmatsu survey on global security said that information security is either part of their strategic direction or that addressing vulnerabilities is a priority. Customer and market demands are driving this focus more than legal or regulatory compliance, yet legislative and regulatory changes may be coming.

In the US, government control over data traffic has typically been opposed in favor of an open Internet and freedom to do business globally, and the tone from Washington may be seen as more cooperative rather than prescriptive. There is a sense that managing cyber risk is an operational activity that companies ought to take on proactively, without requiring Federal legislation. But there is also recognition that a coordinated response between public and private organisations might be a more effective approach to cyber security.

President Obama's recent Executive Order (Feb. 12, 2013) on cyber security paves the way for heightened awareness through identification of critical infrastructure most at risk and improved public-private information-sharing. Depending on whether they fall into a sector deemed at-risk, businesses may face voluntary and mandatory measures to protect the nation's critical infrastructure.

In late 2012, Senator John D Rockefeller sent letters to the chief executives of Fortune 500 companies to engage these enterprises directly on US cyber security practices and build a case for effective legislation. These actions continue the push for more public-private collaboration to better address threats in both sectors.

Already there are interesting initiatives, such as the National Strategy for Trusted Identities in Cyberspace (NSTIC), to address the larger issues of access and identity management at the core of many data security risks.

The increasing velocity and sophistication of attacks isn't the only factor changing the risk equation. The usage paradigm has also changed.

With the increase in third-party relationships (alliances and joint ventures, extensive supply chains and IT, data, and business process-outsourcing) and the surge in mobile and cloud platforms, data is increasingly decentralised. Many businesses are operating in a hybrid environment with many platforms and services, hosted internally and externally, and accessed from multiple end-user devices.

There is no perimeter to defend - boundaries are permeable and data risk must be managed across geographies and organisations. In the Deloitte Touche Tohmatsu security survey, 92 per cent of large companies with more than 10,000 employees, rated security breaches at third-party companies as a concern.

Many companies admit not having or not enforcing contracts or policies to address data security. Similarly, "people" risk - errors and omissions and improper use of consumer technology - represent another large and often overlooked risk, both internally and within third-parties. At the same time, the technology for collecting, storing and sharing data has advanced much faster than the thinking or mechanisms for data security.

A company's call to action

The new era of cyber-security should be both data-driven and data-centric. A security breach isn't a question of "if" but possibly "when". The impact will depend on the industry and the data in question. Understanding how data drives the business is essential to prioritising the risk for different types of data and making decisions about where to invest and how to balance prevention, detection and mitigation efforts.

Look at the business through a data-centric lens: what is the environment, where is the data, how does data move and when, what types of data are collected and how important is the data to the business? Security analytics and automated technological fixes are going to be very important; however, mapping and prioritising the data should come first.

The threat landscape and usage landscape continue to change and companies need to adopt risk management strategies that evolve with the environment. Many companies have trouble with the basics, so a good first step is to start with some simple goals:

Build a true enterprise security program (encompassing IT, business, legal, security, HR, etc.) focused on risk management and leverage technology (the cloud for analytics/reporting, mobile for just-in-time alerting) to be more operationally nimble and informed.

Adopt a strategy for managing risk within business objectives rather than chasing the latest threats and technologies with stop-gap tactics.

Participate in developing and leveraging standards and interacting with public-private initiatives to have a voice in how guidance is developed.

Define and periodically test security requirements for third-parties.

And, engage in public-private and private-private collaboration to share intelligence and form better data security programs within your own network of partners; also, look to the dedicated research feeds and intelligence from security specialists and service providers to enhance and refine your threat analysis.

In some sectors, such as technology, data security efforts may face more resistance because of a prevailing belief that pits openness and innovation against security and protection. However, with the appropriate framework and leadership from the top, innovation can thrive and security and liquidity don’t have to be competing objectives. In fact they may turn out to be a competitive advantage.

Eric Openshaw is a vice chairman and the US Technology, Media & Telecommunications leader for Deloitte and Irfan Saif is a principal and the US Technology, Media & Telecommunications Security & Privacy practice leader at Deloitte & Touche

As used in this document, “Deloitte” means Deloitte LLP and its subsidiaries. Please see ww.deloitte.com/us/about for a detailed description of the legal structure of Deloitte LLP and its subsidiaries. Certain services may not be available to attest clients under the rules and regulations of public accounting.

Reprinted with permission.