InformationWeek DARKReading CONNECTING THE INFORMATION SECURITY COMMUNITY

5/12/2014
12:00 PM

Ted Kobus & Pamela Jones Harbour
Commentary
Connect Directly

8 COMMENTS
COMMENT NOW

Into The Breach: The Limits Of Data Security Technology

When it comes to cyberdefense spending, the smart money should bet on people and compliance as much as on machines.

The relentless assault on American business by cyberthieves has at least two groups spotting a silver lining: entrepreneurs developing new security technologies, and the smart-money folks backing them.

A Wall Street Journal commentary reported recently that investors injected $1.4 billion into cyber security over the past two years, birthing innovative systems that traditional anti-virus software and other passive safeguards can't duplicate.

Companies now have access to new cyberdefense tools deploying shadow networks, virtualization, emulation technology, and other advanced methodologies. But those who deal with data breaches on a regular basis will tell you that technology can only go so far in protecting an organization from intrusion, given the countless human links in the chain of responsibility. To be truly prepared, businesses need to commit to upgrading culture as well as hardware and software. That includes moving away from blind reliance on embedded technology, and doing a better job of managing the unique and changing risks across the enterprise.

A breach is stressful and expensive and only gets worse as word of the attack spreads to employees, customers, shareholders, competitors, and regulators. Today's hackers -- many with global networks and substantial financial resources -- have proven remarkably deft in getting around cyber security. To be properly on alert (as well as compliant with federal and state privacy laws) companies need to conduct periodic cyberrisk assessments, prepare risk management protocols, and educate employees about best-practices for safekeeping sensitive information. A business that doesn't fully

understand its risks can't know which new security system to acquire, or who should be charged with overseeing its privacy function.

Many security breaches are actually the result of low-tech missteps such as improper disposal of sensitive data. In 2009 and 2010, pharmacy chains Rite Aid and CVS were subject to enforcement actions by the Federal Trade Commission when investigations uncovered job applications and prescription labels in publicly accessible dumpsters. In a similar action against American United Mortgage, the FTC found personal loan documents in a dumpster, violating the Gramm-Leach-Bliley Disposal and Safeguards Rule. No big-data program would have saved those companies had identity thieves simply scoured their trash.

Every industry is rushing to elevate standards for storing and disposing of personal information, and for responding to data theft. Chief among those is healthcare, which has seen numerous examples of leaked or stolen patient data. In 2009, a breach notification requirement was added to HIPAA rules governing healthcare providers, requiring them to create internal education programs to raise privacy awareness. Where previously hospitals voluntarily notified patients, now in most circumstances patients must be informed of any data spillage.

Any consumer-facing business is subject to investigations from state attorneys general and the FTC. Financial institutions -- from banks and insurance companies to investment advisors -- must follow practices set forth under Gramm-Leach-Bliley. Universities and schools are governed by the Family Educational Rights & Privacy Act, protecting privacy of student records. Most states now have their own comprehensive privacy laws.

There are numerous steps businesses can take when introducing new products and services, including use of company software that defaults to greater data storage than is required, a review of vulnerabilities in web applications, or elimination of default passwords that are easily penetrated.

Criminals will likely find new ways to circumvent even the smartest systems. Companies should continue their investment in automated tools but mustn't lose sight of the importance of building a strong culture of compliance that focuses on understanding enterprise-wide risks and devising strategies for limiting them.

The FTC remains the primary national regulator of privacy and data security; its settlement agreements and consent decrees are advancing a common law of privacy jurisprudence and also promote codification of best-practices. In a statement marking its 50th Data Security Settlement, the Commission noted that the touchstone of its approach is reasonable security practices by companies, with a focus on compliance and education.

The FTC offers the following principles for implementing reasonable data protection measures:

- Identify what consumer information is collected and which employees or third parties have access to it. Knowing how information moves in and out of an organization is critical to assessing security weaknesses.
- Eliminate needless data storage and unnecessary risk by limiting information collected and retained to legitimate business needs.
- Implement strong employee training and oversight of all service providers.
- Properly dispose of information no longer needed; require vendors to do the same.
- Have a clear plan in place to respond to security incidents.

Corporations have a legal responsibility to demonstrate data security. The law in this area is unsettled and involves different standards, making it difficult to predict liability. Best-practices include raising the level of employee awareness around Internet use, data security, and disposal procedures, and being mindful that unwarranted use of employee or customer information affects every aspect of a company's business. When it comes to shoring up cyberdefenses, the smart money should bet on people and practices as much as on machines.

Ted Kobus focuses his practice in the areas of privacy, data security, and intellectual property. He advises clients, trade groups, and organizations regarding data security and privacy risks, including compliance, developing breach response strategies, defense of regulatory ... View Full Bio