KROLL Fraud Solutions

Kroll's 2011 Data Security Forecast: Top Ten Trends for the Year Ahead

What data security trends can we expect in 2011?

If 2010 is any indication, then regulations, changes in technology, and increasing scrutiny in data privacy and security provide some clues as to what we can expect. And with less than one month to go until the New Year, businesses have no time to waste getting up to speed on the changing risks. Doing so will ensure that they are well-poised for the year ahead. Read on for a 2011 data security forecast from Kroll's Brian Lapidus.

1. We will most likely see an increase in reported, smaller scale breaches. Now that healthcare entities are required to report breaches affecting 500 or more individuals, expect to see more headlines in that industry. Further, as all companies increase data security measures, system audits will bring to light breaches that may have been overlooked in the past. This is not to say that the era of the massive, Heartland or TJX-style breach is over, but they may be matched by small-breach frequency.

2. We'll see more instances of "low-tech" theft, where data is stolen through non-electronic means. Data thieves look for the path of least resistance, focusing on areas of least attention to the organization – and right now, organizations are focused on improving technology, moving from paper to electronic records. So, we can expect to see more low-tech data theft on the horizon – such as the bank teller convicted of identity theft for writing down customer information on sticky notes and using it to open credit accounts.

3. The continuing crisis of lost devices will dominate the data theft landscape. As consumers, we are heavily dependent upon our portable devices – Smartphones, netbooks and laptops. Organizations rely on these devices as well for anytime, anywhere connections. Yet, stolen or missing devices continue to be a major source of data breaches – the US Department of Health and Human Services breach list indicates that 24 percent were due to laptop theft, more than any other specific cause. Expect to see more and more instances and warnings of mobile vulnerabilities and scams – we've already seen an increase in smishing (SMS or text phishing).

4. Data minimization will increasingly be seen as an essential component to data security. Companies that have spent years amassing as much consumer information as possible are starting to view this model as more of a boondoggle than a bounty. If the information is of no use, it represents a liability. In 2011, we will see organizations increasingly turn to data minimization– limiting the data collected and stored, and purging old data on a regular schedule – as a means to reducing their risks.

5. Increasing collaboration and openness will increase vulnerability to data breach. Interoperability is a requirement for healthcare entities switching to electronic health records, but other sectors, like education and government, are increasing initiatives to share and utilize data on a massive scale, as well. By nature, data in transit is data at risk, meaning that the exchange of data opens organizations up to new vulnerabilities — from lackluster data security measures at a partner institution to increased propagation of data.

6. Organizations will increase implementation of social networking policies. For many users, social applications have come to define a large portion of their lifestyle, and they are increasingly bringing their private lives into the

workplace. At the same time, mobile devices have created a world of "24/7" employees, erasing the already fine line between work and home. Employers will need to get a handle on their social networking policies as they relate to data security to ensure that they do not open organizations up to undue risks.

7. Data encryption will be seen as a "golden ticket" to compliance. Encryption is often incorrectly positioned as a complete solution to data security, and new data protection laws in Massachusetts and Nevada continue down this path by making encryption an essential part of organizations' compliance checklists. Companies will have to remember two caveats: compliance doesn't equal data security and encryption doesn't equal a total solution – it is only one tool in the data security arsenal.

8. Third parties will face more stringent breach notification requirements. HITECH is placing business associates under increasing scrutiny, as businesses rely more and more on third party data collection. Expect to see more organizations, even those outside the healthcare industry, placing stringent contractual obligations on their third parties to protect company data.

9. Privacy awareness training will gain prominence as an essential component of breach preparedness. Technology fixes like encryption are effective, but expensive, and electronic monitoring alone won't catch all instances of PII misuse. With comprehensive privacy awareness training, employees can act as privacy advocates who know how to recognize security hotspots, understand legal obligation, and use vigilance whenever they deal with PII. This is the kind of security equity that no technology can buy.

10. The possibility of a federal breach notification law is high for 2011. While it's difficult to go out on a limb and claim we'll definitely see a law in 2011, there are some compelling reasons why an overarching federal law is on the horizon:

- States are moving forward, creating a confusing tapestry of conflicting law. A federal law would cut through the noise.
- Congress has enacted considerable legislation recently — namely HITECH — that opens the door to further legislation.
- Through grants and other funding sources, the federal government is continuing an aggressive path to encourage the growth of technological initiatives (such as the ONC Beacon grants and the USDOE's Race to the Top). These new initiatives require new ways of thinking about data security and privacy.

Kroll's Fraud Solutions
866 419 2052
www.krollfraudsolutions.com
www.kroll.com