For Security & Risk Professionals

January 9, 2009

Top Data Security Predictions For 2009

Economic Turmoil Will Increase Need For Surveillance, Data Protection Tools

by Andrew Jaquith and Natalie Lambert

with Andras Cser, Stephanie Balaouras, and Alex Crumb

**EXECUTIVE SUMMARY**

The economic turmoil in the United States will have resounding consequences for security and risk professionals in 2009. The prospect of laying off an additional 1.4 million workers means that CISOs will clamor for data protection tools to keep their confidential data from walking out the door. These same managers will purchase full-disk encryption and device control technologies and push them enterprisewide while continuing to delay deployment of enterprise rights management (ERM) software. Meanwhile, reforms to the US healthcare system and the illicit leaks of customer personally identifiable information (PII) will escalate the issue of access entitlements to the corner office. Finally, Forrester predicts that client virtualization will move into the early majority phase as enterprises look to alternative ways to protect their PC data.

**EMPLOYEE LAYOFFS STOKE FEARS OF DATA THEFT, IGNITE SALES**

2008 was a year of severe turmoil for North American enterprises. Problems initially confined to the subprime loan market infected the broader financial services, which in turn rippled outward to the construction, retail, and transportation industries. The deepening financial crisis in the US has led to mass layoffs by employers: 530,000 in November alone.

Employers laying off workers will clamor for data protection tools... With the global recession likely to last another five to seven quarters, even relatively healthy enterprises will be under pressure to shed workers. The U.S. Federal Reserve estimates that the unemployment rate will rise to 7.1% to 7.6% in 2009, implying future job losses of another 600,000 to 1.4 million.

CISOs at affected firms in the United States, Europe, and elsewhere will be handed a clear mandate by their bosses: Keep the data from walking out the door when their employees do. What will this mean? Forrester believes that increased diligence regarding account and directory deprovisioning will be one natural consequence. The faster affected workers' entitlements can be revoked after the layoff, the better.

While faster deprovisioning will help with employees who have been let go, in 2009 data protection tools will be seen as a critical technology for limiting the loss of sensitive information before layoffs happen. Employers will buy data leak prevention (DLP), device control, and Web filtering technologies to help them clamp down on nervous employees sending themselves attachments to outside Webmail addresses, block bulk copying to USB thumb drives, and monitor postings to outside blogs. As a result, we expect employment pressures to help data security vendors exceed the overall market growth for security products and tools in 2009.
Top Data Security Predictions For 2009
For Security & Risk Professionals

... But Most Purpose-Built DLP Deployments Will Fail To Move Beyond The Pilot Stage

With cutbacks to their workforces looming, executive sponsorship (of DLP tools in particular) will be strong enough to ensure that they stay in the 2009 budget. Forrester expects that the percentage of North American companies deploying DLP will rise to 60% by the end of 2009, up from 39% in 2008.6

However, DLP deployments to date have been small, both in scope of deployment and scope of features used. CISOs Forrester spoke to indicate that DLP — today — solves narrow problems, like limiting inadvertent disclosure of credit card numbers, government identifiers, and bulk customer lists. But few organizations use DLP to find more ethereal and strategic information like sales contacts, product plans, or earnings forecasts — exactly the sort of valuable assets that nervous employees might be tempted to squirrel away. What's more, the newer features of DLP tools, like blocking postings to external blogs and wikis, aren't widely used yet.

Forrester’s burning question for 2009 is: Will DLP tools finally get past the hype and help employers safeguard their most valuable intellectual property? Our answer is a qualified "yes." Although DLP vendors will close record numbers of deals in 2009, value won't come as quickly as enterprise CISOs might like. Once started, enterprises take several quarters to achieve meaningful value with DLP. Deployments will stay small until at least 2010, when enterprises move beyond simple credit card filtering rules and USB port blocking.

The Majority Of Large Corporations Will Deploy Full-Disk Encryption For Laptops

If DLP is the enterprise CISO’s precision instrument — one that finds needles in haystacks — full-disk encryption is the security blanket — the safe, comfortable measure that allows the CISO to sleep at night. Full-disk encryption's goal isn't to protect against dissemination of specific documents. Rather, it protects the entire contents of a worker's computer in the event of theft or loss. In most cases, this means that organizations will not have to disclose a data breach. Time-to-value for full-disk encryption is relatively rapid, because IT can deploy the software with minimal customization.

Motivated by the fear of a toxic data spill like the one that affected the Department of Veterans Affairs in May 2006, enterprises have been buying security blankets by the bagful. Of 500 very large enterprises Forrester surveyed, 35% have already deployed full-disk encryption. Another 19% will deploy in 2009.7 We expect that by 2011, three-quarters of large and very large enterprises will make full-disk encryption a standard part of their PC builds. The inclusion of BitLocker into enterprise versions of Windows Vista and Windows 7 will help drive adoption . . . but only at companies that have already planned to replace existing hardware.

Headlines Will Transform Entitlement Management Into A CEO-Level Concern

As most security and risk professionals know, abuse of privileges by authorized insiders with excessive privileges (entitlements) is more worrying than theft of data by outsiders.8 But problems
caused by excessive entitlements haven't generated nearly as much buzz in the corner office as have stories about data loss and theft. Headlines about lost backup tapes, infected USB sticks, and absentminded Veterans Affairs staffers make for great copy. CEOs understand outsider risks quite well. Much harder to understand have been stories about how crafty Société Générale trader Jerome Kerviel could exploit esoteric knowledge of trading and back-office processes to cause his employer to lose $7 billion. The root causes, though hard to capture in newspaper sound bites, are straightforward: excessive application privileges, lack of separation of duties between roles, and failure to remove access to applications when employees take new positions within the company.

In 2009, entitlements will give CEOs major headaches. A familiar toxin will cause the discomfort: PII about customers. Except that this time, insiders with too many privileges will be the cause, not outsiders or opportunists chancing upon lost laptops. Customer PII will ensure that entitlement management will become a CEO-level concern in 2009. Drivers will include:

- **Employee curiosity.** In November, Verizon Wireless fired several employees for sharing the cell-phone records of President-elect Barack Obama. Contrary to early reports, the employees did not hack Obama’s account — they merely used privileges they already possessed. Forrester predicts that more high-profile stories about unauthorized snooping will become much more common next year. If 2006 was “The Year of the Lost Laptop,” 2009 will be “The Year of the Curious Customer Service Representative.”

- **Quick money.** Customer information used to manufacture identities and open credit continues to be valuable. Recent security intelligence from Symantec, for example, states that underground prices for consumer credit card details range from $0.50 to $12 per card. By that measure, an entitled employee with excessive privileges at an online merchant with sloppy internal controls could sell 10,000 card numbers and make a quick $100,000.

- **Wide-open healthcare records.** With the Obama administration expected to unveil major reforms to the US healthcare system, interoperability and access control of electronic personal health records will become a significant priority. Spirited and public debates over who can access patient records, and under what circumstances, will drive greater awareness of entitlements in healthcare, life sciences, and beyond.

- **Smarter auditors.** Few organizations implement entitlement review and recertification processes unless auditors force them to. As auditors have gained more experience assessing compliance with Sarbanes-Oxley and other statutes, they have become increasingly aware of the perils of excessive entitlements. Greater awareness has led to tougher audits. Now enterprises must be prepared to explain who got access to what application features, and why.

Forrester expects that these high-level drivers will drive enterprises to take a much closer look at products that discover, report on, and periodically recertify employee entitlements, although budget constraints will limit significant adoption until 2010.
**Enterprise Rights Management Won’t Go Mainstream In 2009 . . .**

In the fourth quarter of 2008, ERM and DLP vendors announced several deals that portend increased integration between the two categories. In December, Microsoft announced that it had licensed RSA’s content classification technology for inclusion with Microsoft’s Active Directory Rights Management Server (RMS). A few days later, McAfee announced that it would integrate its DLP Discover and DLP Prevent products with Liquid Machines’ Gateway for DLP. Although the deals differ in the details, they show how data labeling and data filtering are two sides of the same coin. ERM labels information upfront and protects information according to declarative policies; DLP classification engines seek to retroactively categorize information that wasn’t labeled to begin with.12

The Microsoft/RSA and McAfee/Liquid Machines deals are great news for customers who have ERM deployments already or are seeking to buy ERM in the near future. The trouble is, it’s a small buying pool. Forrester receives very few inquiries from enterprise customers about ERM, and customers who have it aren’t using it in large-scale deployments.

Forrester predicts that just like 2008 wasn’t the year of ERM, 2009 won’t be either. Enterprises will continue to derive value from ERM deployments that protect specific and narrowly defined information assets like earnings forecasts and product plans. But in the current economic climate, enterprises that don’t have it will see ERM for what it is: an expensive, nice-to-have niche technology with complex deployment requirements.

. . . But Client Virtualization Will Be Adopted By Many More Enterprises

Hosted application and desktop virtualization technologies, such as those from Citrix, Microsoft, and VMware, have long been used to address remote access and manageability concerns.13 However, in 2008, Forrester clients told us that the majority of new client virtualization deployments were justified with an entirely different but sensible reason — securing data on the user PCs. This trend will continue strongly into 2009.

The business case for client virtualization has never been easy, but increased data security concerns will make virtualization much more palatable to CIOs in 2009, even in the midst of a difficult economic climate. Why? In short, because enterprises will see client virtualization increasingly as a dual-use technology that can increase productivity and security at the same time. Hosted virtualization technologies enable users to access their applications or desktops from any device with a network connection, while at the same time keeping sensitive data stored in the safety of the data center.

Forrester expects that CISOs in vertical markets with stringent data security requirements will move rapidly to full-blown deployments. Historically, highly regulated industries such as healthcare and financial services adopted client virtualization first because of the clear linkages to security.
Throughout 2009, increased turnover in employee ranks will offer further justification to these and other industries, based on client virtualization’s potential for decreasing the possibility of data breaches. As a result, data security will continue to be the No. 1 driver of client virtualization initiatives through 2011.

ENDNOTES

1 The question for the US tech market is no longer whether the US economy is in recession — instead, it is how long and deep the recession will be and how much damage will it do to the tech sector. See the December 9, 2008, “US IT Market Outlook: Q4 2008” report.


4 According to the economic projections of the Board of Governors of the Federal Reserve System and presidents of the Federal Reserve Banks, the 2009 unemployment rate is expected to rise to 7.1% to 7.6%. Assuming a constant labor force size, this implies that in 2009 11.0 million to 11.8 million US citizens will be unemployed. What it means: 646,000 to 1,420,000 additional workers will lose their jobs. Source: FRB: “Summary of Economic Projections,” October 28-29, 2008 (http://www.federalreserve.gov/monetarypolicy/fomcminutes20081029ep.htm).

5 Forrester evaluated leading data leak prevention (DLP) vendors across approximately 74 criteria and found that Websense and Reconnex came out on top because of their strong go-to-market strategy and automated learning capabilities, respectively. See the June 6, 2008, “The Forrester Wave™: Data Leak Prevention, Q2 2008” report.


7 Source: Forrester’s Q3 2008 Combined SMB And Enterprise IT Security Study Survey.

8 IT security and risk management professionals preach the principle of least privilege: Employees who do not need access to particular documents and data records shouldn’t get it. Wall Street investment banks, for example, have incorporated the concept of “entitlements” — the enumeration of each employee’s information access needs — into their programs. More recently, statutes like Sarbanes-Oxley and IT security standards like ISO 27001 have stressed the importance of regularly reviewing employee entitlements as part of a well-balanced identity and access management program.

Top Data Security Predictions For 2009
For Security & Risk Professionals

Forrester Research, Inc. (Nasdaq: FORR) is an independent research company that provides pragmatic and forward-thinking advice to global leaders in business and technology. Forrester works with professionals in 19 key roles at major companies providing proprietary research, consumer insight, consulting, events, and peer-to-peer executive programs. For more information, visit www.forrester.com.

© 2009, Forrester Research, Inc. All rights reserved. Unauthorized reproduction is strictly prohibited. Information is based on best available resources. Opinions reflect judgment at the time and are subject to change. Forrester®, Technographics®, Forrester Wave, RoleView, TechRadar, and Total Economic Impact are trademarks of Forrester Research, Inc. All other trademarks are the property of their respective companies. To purchase reprints of this document, please email clientsupport@forrester.com. For additional information, go to www.forrester.com.


12 Despite years of investments in technology and processes, protecting enterprise-wide data remains a maddeningly elusive goal for chief information security officers (CISOs). See the January 5, 2009, “Data-Centric Security Requires Devolution, Not A Revolution” report.

13 To virtualize or not to virtualize? That is no longer the question. See the April 9, 2008, “Demystifying Client Virtualization” report.