July 12, 2012

Kill Your Data To Protect It From Cybercriminals

by John Kindervag
for Security & Risk Professionals

FORRESTER® Making Leaders Successful Every Day

July 12, 2012

Kill Your Data To Protect It From Cybercriminals

Strategic Plan: The Data Security and Privacy Playbook

by John Kindervag
with Stephanie Balaouras and Jessica McKee

EXECUTIVE SUMMARY

As cybercriminals have become more skillful and sophisticated, they have eroded the effectiveness of our traditional perimeter-based security controls. The constantly mutating threat landscape requires new defensive measures, one of which is the pervasive use of data encryption technologies. In the future, you will encrypt data — both in motion and at rest — by default. This data-centric approach to security is a much more effective way to keep up with determined cybercriminals. By encrypting, and thereby devaluing, your sensitive data, you can make cybercriminals bypass your networks and look for less robustly protected targets. Encryption will become a strategic cornerstone for security and risk (S&R) executives responsible for their organization's data security and privacy efforts. We designed this report to help you understand how to use encryption, tokenization, and other technologies to "kill your data."

TABLE OF CONTENTS

NOTES & RESOURCES

In developing this report, Forrester drew from a wealth of analyst experience, insight, and research through advisory and inquiry discussions with end users, vendors, and regulators across industry sectors.

Related Research Documents

"The Future Of Data Security And Privacy: Controlling Big Data"
January 26, 2012

"Rethinking DLP"
January 3, 2012

"Introducing Forrester's Data Privacy Heat Map"
December 22, 2011

IF THEY CAN'T SELL IT, THEY WON'T STEAL IT

There are two types of data: data someone wants to steal and everything else. Most security professionals today do not understand the motivations behind data theft; they put controls in place that protect the data that is most valuable to them, as opposed to data that is most valuable to criminals. This means that control placement is often flawed and security pros frequently leave toxic data, data associated with legal or compliance mandates, and certain types of intellectual property unprotected and vulnerable.

Traditionally, security pros have not stored email addresses in an encrypted format — because they don't view them as toxic or sensitive data. The Epsilon email data system breach in April 2011 answered the question of whether email addresses are valuable data with a resounding "Yes." This breach demonstrated the value of stolen email addresses and the need for security and data stewardship best practices in dramatic fashion.[1] Cybercriminals compromised a marketing database containing email addresses from more than 100 companies.[2] The breach affected tens of millions of consumers, whose email addresses are now in the hands of potential malevolent actors.[3] There are real fears that this breach, and others like it, will result in an increase in targeted spear phishing attacks. During a spear phishing attack, cybercriminals carefully craft emails enticing users to click on a malicious link or unwittingly download malware. It's often difficult for even the most security-conscious users to identify these emails as malicious.[4] For example, the security vendor RSA admitted that its highly publicized and damaging breach was the result of a phishing attack.[5] There are some indications that cybercriminals targeted RSA in order to attack certain defense contractors that relied on RSA's two-factor authentication methods.[6]

Encryption Prevents Cybercriminals From Monetizing Your Stolen Data

In order to properly protect data, security professionals must put a value on it based on how much the data is worth on the open market. There is a market for stolen data such as credit cards, credit reports, certain types of intellectual property, and personally identifiable information (PII) such as Social Security Numbers. This underground economy is based on the principles of supply and demand — just like any other market. Hackers who steal this data can sell it on underground auction sites (the cybercriminals' equivalent of eBay) or to direct data brokers — think of them as cyberspace fences. These markets exist in IRC chat rooms or on carder websites out on the invisible Internet — the part of the Web that the rest of the world doesn't see but which exists to monetize data.[7] Your goal, then, is to devalue or "kill" data. As a general rule, cybercriminals cannot sell encrypted data in the open markets on the invisible Internet; encrypted data has no value, thus destroying malicious actors' primary incentive to steal it.

Encryption Covers A Multitude Of Sins

Ubiquitous encryption is the only hope we have of maintaining some kind of parity with attackers in the new threat landscape. Not only does encryption devalue the data from the attacker's perspective, it generally places that data outside the scope of compliance regimes like PCI or US state privacy

laws.[8] California's privacy law, SB 1386, set the precedent for this; the law was the first of its kind and most other state governments derived their own privacy laws from it. According to SB 1386, only unencrypted PII is subject to the law.[9]

One good example of the effectiveness of encryption in shielding an organization from compliance penalties is the Sony PlayStation Network (PSN) breach. In April 2011, Sony PSN suffered a significant breach, in which cybercriminals compromised the records of approximately 77 million subscribers.[10] Sony said that it had encrypted credit card data; it wouldn't confirm that any of this data was stolen, but stated that "While there is no evidence at this time that credit card data was taken, we cannot rule out the possibility."[11] Although it's likely that encrypted credit card data *was* among the big chunks of stolen data, as these types of attacks are generally indiscriminate and designed to grab as much data as possible, the attackers would have been unable to monetize any encrypted credit card data without the keys to decrypt it. Encrypted data in the absence of keying material is useless — it's not really data at all.

Key Management Holds The Key To Killing Data

While the implementation of encryption is complex, conceptually it is easy to understand. The final encrypted solution has two parts: the encrypted data itself and the keys that control the encryption and decryption processes. Controlling and maintaining the keys, therefore, is the most important part of an enterprise encryption strategy. Encryption methods and algorithms are standardized and well understood, but key management is unique to each organization.[12] This is where enterprise encryption becomes tricky — and why key management holds the key to killing data.

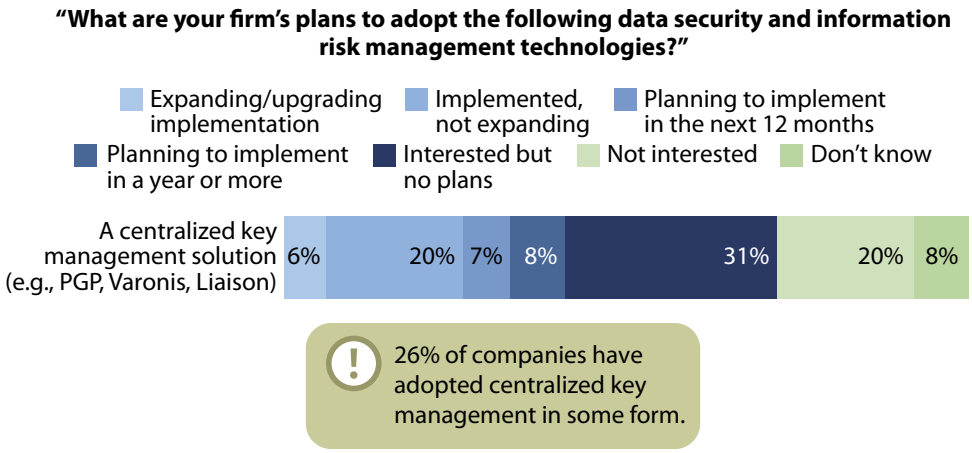
Effective key management must include processes for distributing, escrowing, and revoking keys, among many other functions. Many organizations have key management solutions as part of the cryptographic subsystems they use, such as email encryption, database encryption, and desktop and laptop encryption. However, most security professionals manage these applications — and the keys associated with them — individually. As the need for more widespread encryption becomes the norm, look for enterprises to try to aggregate key management into a centralized solution. Today, approximately 26% of companies have adopted centralized key management in some form (see Figure 1). In the future, expect the demand for enterprise key management to grow because:

- **Key management is necessary for mobile device certificate management.** Not only do security professionals need the keys that control encryption, they also need the same type of systems to manage the X.509 certificates that they will deploy to authenticate mobile devices such as smartphones and tablet computers.[13]

- **Key management standardization is well underway.** There are a number of efforts in motion to standardize enterprise key management processes. The US National Institute of Standards and Technology (NIST), for example, is working on a set of guidelines that are highly influential in the cryptographic community.[14] Additionally, a consortium of encryption vendors is

working to create the key management interoperability protocol (KMIP).[15] KMIP promises to allow organizations to manage diverse cryptographic subsystems via a single enterprise key management application.

Figure 1 Centralized Key Management Adoption



Base: 1,052 North American and European executives and technology decision-makers

Source: Forrsights Security Survey, Q2 2011

61298 Source: Forrester Research, Inc.

Other Data-Killing Technologies Can Uplift Data Security

Encryption is not the only technology that can deal a death blow to toxic data. Other data extraction solutions, such as tokenization and data masking, can provide value by rendering certain data strings unreadable. This is especially useful in obfuscating information like Social Security Numbers in data containers where encryption is not an option. More specifically:

- **Tokenization abstracts data to protect it.** Data strings such as credit card numbers are widely tokenized in order to meet PCI requirements. The token is a string of characters that exists in an application or data store and serves as a placeholder for the data string, avoiding the inherent risk of storing the original toxic data string. PCI has taught information security pros how to tokenize data economically and at scale.[16]

- **Data masking is useful for test data.** To test functionality and upgrades, application developers need a test database populated with "real" data. However, exposing real PII to developers can violate privacy laws. Data masking conceals real data by scrambling it to create a new data string, scrubbing the string of identifying information but retaining the properties of the original data so that you can keep it in existing data stores. Once stripped of the personal identification, the data falls outside the scope of most privacy laws.[17]

- **Defensible disposal of data prevents criminals from using it against you.** The periodic and permanent destruction of unneeded data will become an integral part of the data-killing process. Most organizations never touch a significant proportion of the vast amount of the data they store. Absent a true business or compliance mandate to retain this data, you should defensively dispose of it so it will no longer tempt malicious actors.[18]

ENCRYPTION ALREADY EXISTS THROUGHOUT TODAY'S ENTERPRISE

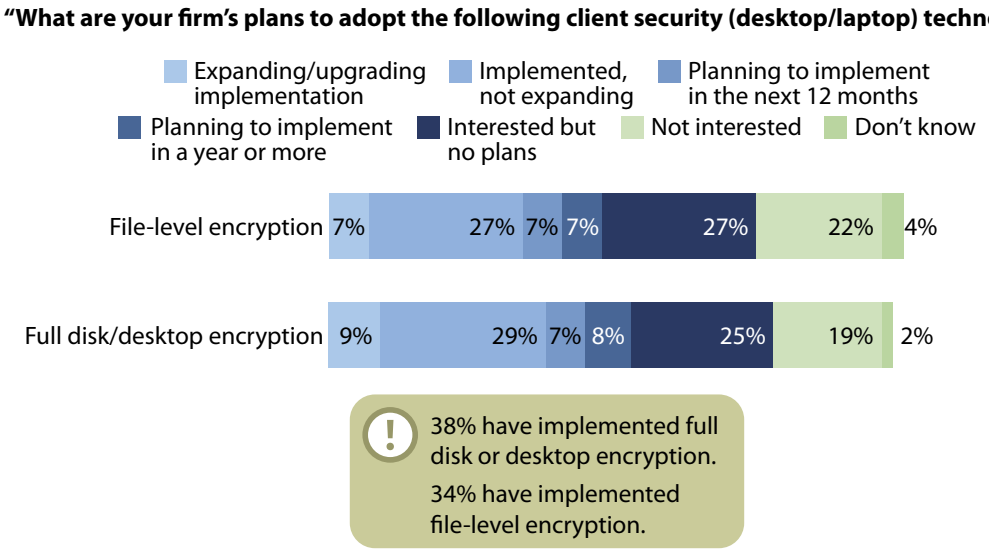
Security pros have deployed a wide variety of cryptographic solutions in most modern networks. These include the widespread encryption of hard drives on desktops and laptops, the encryption of emails containing sensitive information, and the continuing adoption of database encryption.

Endpoint Encryption Solutions Are Common

Adoption of endpoint encryption for laptops and desktops is a widespread and accepted practice in enterprises today. There are two methods of endpoint encryption: full disk and file-level encryption. Full disk encryption encrypts the entire hard drive, whereas file-level encryption only encrypts the portion of the drive where sensitive information is stored. The adoption rates of these technologies are nearly equal; 38% of companies have chosen to implement full disk or desktop encryption, while 34% have implemented file-level encryption (see Figure 2).

Look for adoption to increase as more companies buy machines with self-encrypting drives. This new hard disk technology performs the encryption in the hardware itself. While there is still a need for encryption management software, self-encrypting drives promise improved cryptographic performance, thus eliminating one of the final barriers to adopting client encryption.

Figure 2 File-Level And Full Disk Encryption Adoption



Base: 1,282 North American and European executives and technology decision-makers (percentages do not total 100 because of rounding)

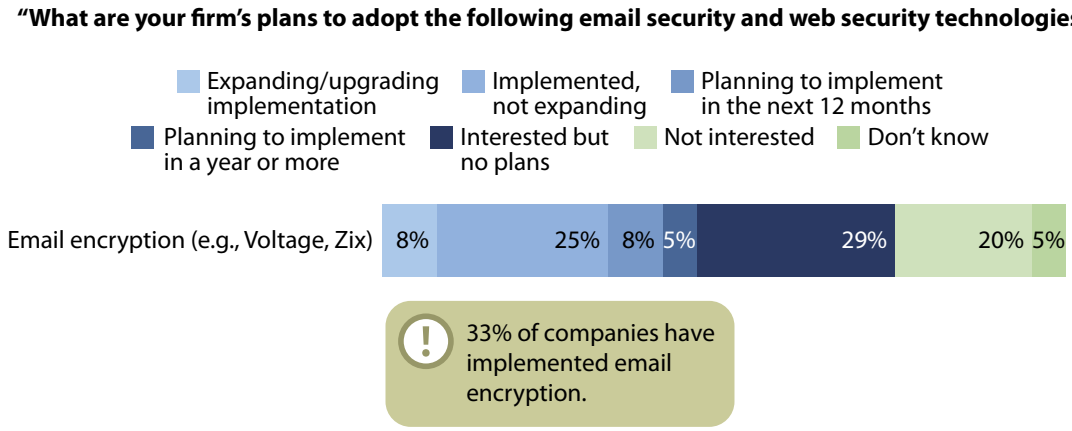
Source: Forrsights Security Survey, Q2 2011

61298 Source: Forrester Research, Inc.

Email Encryption Is A Mainstay Of Many Compliance-Driven Organizations

Compliance initiatives such as PCI and the HIPAA and HITECH Acts all but mandate email encryption. For example, the transmission security standard of HIPAA Security Rule section 164.312 states: "Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network."[19] The only way to effectively meet this standard is to encrypt emails that contain sensitive information. In 2011, 33% of companies Forrester surveyed indicated that they have implemented email encryption (see Figure 3).

Figure 3 Email Encryption Adoption



Base: 1,282 North American and European executives and technology decision-makers

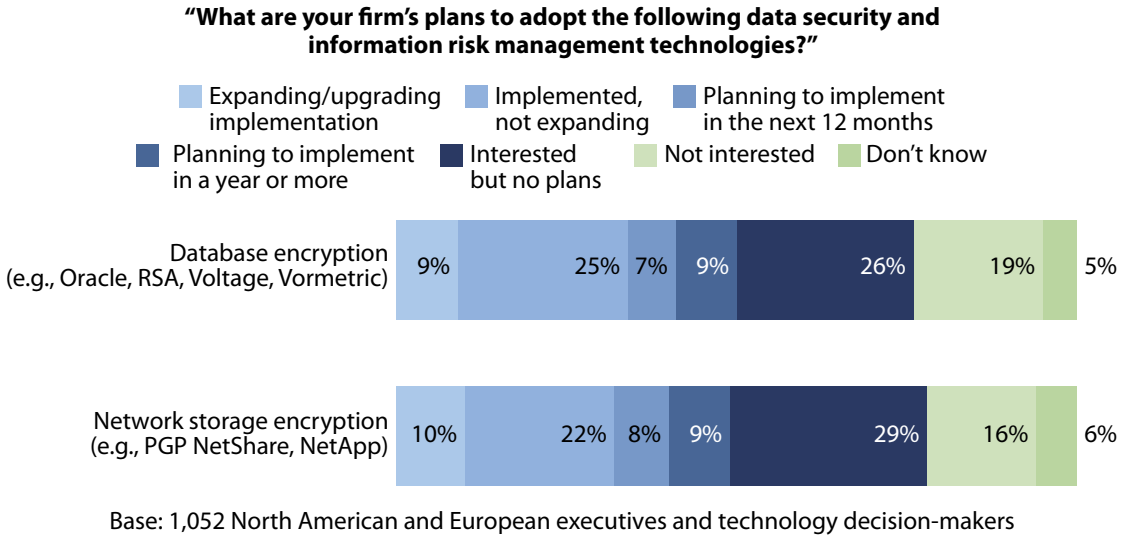
Source: Forrsights Security Survey, Q2 2011

61298 Source: Forrester Research, Inc.

Database And Network Data Storage Encryption Are Becoming More Common

Compliance mandates and privacy laws have given companies incentives to deploy more and more encryption. As sensitive data very often resides in enterprise databases, it is no surprise that encryption of storage and databases is becoming more common. Network storage encryption had a 32% adoption rate and database encryption had a 34% adoption rate in Forrester's most recent security survey (see Figure 4).

Figure 4 Network Storage And Database Encryption Adoption



Base: 1,052 North American and European executives and technology decision-makers

Source: Forrsights Security Survey, Q2 2011

61298 Source: Forrester Research, Inc.

YOU DON'T HAVE TO BE A CRYPTOGRAPHER TO USE ENCRYPTION

A noteworthy inhibitor of encryption is an unfounded — and unhealthy — fear of cryptographic technologies. Too many security pros focus on the technology behind encryption, such as the encryption algorithms themselves. There is a misconception that you need to be a mathematician or a cryptographer to properly deploy cryptographic solutions. In reality, good encryption is all about abstraction and management. The widespread use of SSL/TLS is a good example: This cryptographic solution undergirds the Internet and our eCommerce systems, but the technical details are transparent to the individuals who deploy it. SSL/TLS is now so mainstream that we typically don't spend much time thinking about its complexity. Other cryptographic solutions will evolve in a similar manner; sometime in the near future we will find that we encrypt almost all of our data and will be surprised when we find unencrypted data in our organizations.

RECOMMENDATIONS

IT'S ALL ABOUT THE DATA

Few business processes today are not IT-enabled. Whether it's the rollout of new products and services, geographic expansion, acquisitions, creative marketing campaigns, or business intelligence initiatives, your organization is generating, collecting, and storing huge amounts of data — think petabytes. Much of that data will be sensitive or toxic. Much of that data will make

attackers salivate. The only way to properly secure and devalue this data will be to encrypt or otherwise abstract it. As you formulate your encryption strategy, keep in mind that:

- **Mobility will drive new data-killing initiatives.** The advent of the extended enterprise and the ease of accessing corporate information anytime, anywhere, and on any device will create new pressures on security teams to encrypt data. Mobile devices are easy to lose and easy to steal. Enterprise-level encryption is the best hope for securing data on these devices.
- **Encryption is a type of data loss prevention.** Data is the lifeblood of the modern corporation. Not only can data breaches damage us from a legal or compliance perspective, intellectual property theft damages an enterprise's competitive edge. By encrypting data, you protect it from leaking, as leaked encrypted data cannot harm you if you properly manage the keys.
- **Thoughtful use of encryption lessens data privacy and residency issues.** Many countries have enacted data privacy regulations stipulating the conditions under which organizations can collect personal data; these regulations further outline the measures to safeguard that data and the requirements for and limitations on international data transfer. Privacy laws have impeded the adoption of managed and cloud-based services and forced many organizations to rearchitect their networks and change the location of their data centers. The judicious use of encryption and other data-killing technologies can help you meet cross-border security demands.
- **Encryption will become critical in multitenant cloud security.** Business and IT leaders alike are eager to adopt cloud computing to reduce IT costs, provide scale, and enable more flexibility. But cloud computing leads to unique data segregation issues, because providers often use virtualization technology to host multiple tenants on shared IT infrastructure. In fact, this multitenacy is the cornerstone of cloud economics. However, many security professionals are uncomfortable with multitenancy — and for good reason. In a multitenant environment, data encryption holds the best hope of properly protecting commingled data.

SUPPLEMENTAL MATERIAL

Methodology

Forrester's Forrsights Security Survey, Q2 2011, was fielded to 2,353 IT executives and technology decision-makers located in Canada, France, Germany, the UK, and the US from small and medium-size business (SMB) and enterprise companies with two or more employees. This survey is part of Forrester's Forrsights for Business Technology and was fielded during June 2011. LinkedIn Research Network fielded this survey online on behalf of Forrester.

Forrester's Forrsights Security Survey, Q3 2010, was fielded to 2,337 IT executives and technology decision-makers located in Canada, France, Germany, the UK, and the US from SMB and enterprise companies with two or more employees. This survey is part of Forrester's Forrsights for Business Technology and was fielded from May 2010 to July 2010. LinkedIn Research Network fielded this survey online on behalf of Forrester.

Forrester's Enterprise And SMB Security Survey, North America And Europe, Q3 2009, was fielded to 2,199 IT executives and technology decision-makers located in Canada, France, Germany, the UK, and the US from SMB and enterprise companies with two or more employees. This survey is part of Forrester's suite of Business Data Services studies. Forrester fielded the survey from August 2009 to September 2009. LinkedIn fielded this survey online on behalf of Forrester.

Each calendar year, Forrester's Forrsights for Business Technology fields business-to-business technology studies in more than 17 countries spanning North America, Latin America, Europe, and developed and emerging Asia. For quality control, we carefully screen respondents according to job title and function. Forrester's Forrsights for Business Technology ensures that the final survey population contains only those with significant involvement in the planning, funding, and purchasing of IT products and services. Additionally, we set quotas for company size (number of employees) and industry as a means of controlling the data distribution and establishing alignment with IT spend calculated by Forrester analysts. Forrsights uses only superior data sources and advanced data-cleaning techniques to ensure the highest data quality.

We have illustrated only a portion of survey results in this document. To inquire about receiving full data results for an additional fee, please contact forrsights@forrester.com or your Forrester account manager.

Companies Interviewed For This Document

Dell
IBM
I Think Security
McAfee
PKWare
Protegrity
RSA
SafeNet
Symantec
Thales
Trend Micro
Voltage Security
Vormetric
Wave Systems

ENDNOTES

[1] For more information, see the September 23, 2011, "Work With Marketing Pros To Prevent Breaches" report.

[2] On April 1, 2011, Epsilon issued a terse press release about the breach. Source: "Epsilon Notifies Clients Of Unauthorised Entry Into Email System," Epsilon press release, April 1, 2011 (http://www.epsilon.com/emea/news-events/press-releases/2011/epsilon-notifies-clients-unauthorised-entry-email-system-0).

[3] A list of compromised companies can be found on the DataBreaches website. Source: "And The Hits Just Keep On Coming For Epsilon," DataBreaches.net, April 3, 2011 (http://www.databreaches.net/?p=17374). The Privacy Rights Clearinghouse estimates that between 50 million and 250 million email addresses were stolen. Source: "Data Breaches: A Year in Review," Privacy Rights Clearinghouse, December 16, 2011 (https://www.privacyrights.org/top-data-breach-list-2011). The exact number is unknown.

[4] Multiple news reports have articulated concerns about an increase in phishing attacks. Source: Brian Krebs, "Epsilon Breach Raises Specter Of Spear Phishing," *Krebs On Security Blog*, April 4, 2011 (http://krebsonsecurity.com/2011/04/epsilon-breach-raises-specter-of-spear-phishing/) and Fahmida Rashid, "Epsilon Breach A Treasure Trove For Phishing Attacks," eWeek.com, April 4, 2011 (http://www.eweek.com/c/a/Security/Epsilon-Breach-a-Treasure-Trove-for-Phishing-Attacks-845293/).

[5] Details about the RSA attack have been widely published. Source: Uri Rivner, "Anatomy Of An Attack," *RSA Speaking Of Security Blog*, April 1, 2011 (http://blogs.rsa.com/rivner/anatomy-of-an-attack/) and Kim Zetter, "Researchers Uncover RSA Phishing Attack, Hiding In Plain Sight," *Wired Threat Level Blog*, August 26, 2011 (http://www.wired.com/threatlevel/2011/08/how-rsa-got-hacked/).

[6] There is much speculation that there is a direct link between the RSA breach and the breaches (or attempted breaches) of defense contractors. Source: Jim Finkle and Andrea Shalal-Esa, "Exclusive: Hackers Breached U.S. Defense Contractors," Reuters, May 27, 2011 (http://www.reuters.com/article/2011/05/27/us-usa-defense-hackers-idUSTRE74Q6VY20110527) and Elinor Mills, "Report: Data Stolen In RSA Breach Used To Target Defense Contractor," CNet, June 1, 2011 (http://news.cnet.com/8301-27080_3-20068051-245.html).

[7] A recent Bloomberg report provided more information on these underground markets. Source: Michael Riley, "Stolen Credit Cards Go For $3.50 At Amazon-Like Online Bazaar," Bloomberg, December 20, 2011 (http://www.bloomberg.com/news/2011-12-20/stolen-credit-cards-go-for-3-50-each-at-online-bazaar-that-mimics-amazon.html).

[8] For more information on privacy laws, see the April 21, 2011, "The Privacy Almanac Series: Establishing A Privacy Framework" report and see the December 22, 2011, "Introducing Forrester's Data Privacy Heat Map" report.

[9] California SB 1386 states that "This bill, operative July 1, 2003, would require a state agency, or a person or business that conducts business in California, that owns or licenses computerized data that includes personal information, as defined, to disclose in specified ways, any breach of the security of the data, as defined, to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person." Source: California State Senate (http://info.sen.ca.gov/pub/01-02/bill/sen/sb_1351-1400/sb_1386_bill_20020926_chaptered.html).

[10] More details on the Sony PSN breach can be found in the DataLossDB website. Source: DataLossDB (http://datalossdb.org/incidents/3634-77-million-names-addresses-email-addresses-birthdates-playstation-network-qriocity-passwords-and-logins-handle-psn-online-id-profile-data-purchase-history-and-possibly-credit-cards-obtained).

[11] Sony maintains a site about the PSN breach. Source: "Q&A #1 For PlayStation Network And Qriocity Services," *PlayStation Blog* (http://blog.us.playstation.com/2011/04/27/qa-1-for-playstation-network-and-qriocity-services/).

[12] NIST is considered the keeper of approved cryptographic algorithms. It has created a document store called the "Cryptographic Toolkit." NIST's recommendations, therefore, are considered the de facto standards of cryptography. Source: National Institute of Standards and Technology (http://csrc.nist.gov/groups/ST/toolkit/index.html).

[13] For a discussion of certificate-based authentication, see the January 6, 2011, "Identity And Access Management Predictions: 2011 And Beyond" report.

[14] NIST publications on key management include these reports. Source: Elaine Barker, William Barker, William Burr, William Polk, and Miles Smid, "Recommendation For Key Management," NIST, May 2011 (http://csrc.nist.gov/groups/ST/toolkit/documents/SP800-57Part1-Revision3_May2011.pdf) and Elaine Barker, Dennis Branstad, Santosh Chokhani, and Miles Smid, "A Framework For Designing Cryptographic Key Management Systems," NIST, June 15, 2010 (http://csrc.nist.gov/publications/drafts/800-130/draft-sp800-130_june2010.pdf).

[15] The Organization for the Advancement of Structured Information Standards provides information on Oasis key management interoperability protocol (KMIP) solutions. Source: Oasis (http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=kmip).

[16] For more information on tokenization and data masking, see the April 7, 2010, "Demystifying Tokenization And Transaction Encryption, Part 1: Get Ready To Place Some Bets" report and see the April 15, 2010, "Demystifying Tokenization And Transaction Encryption, Part 2: When To Double Down" report.

[17] For more information and recommendations on data security trends and drivers, current data security challenges, why data masking is critical, approaches to data masking, and selection criteria for data masking implementations, see the July 9, 2009, "Why Data Masking Should Be Part Of Your Enterprise Data Security Practice" report.

[18] For more information, see the January 29, 2009, "Inquiry Spotlight: Records And Retention Management, Q1 2009" report.

[19] The full text of HIPAA Security Rule Section 164.312 (e)(1) is available on the US Government Printing Office website. Source: US Government Printing Office (http://edocket.access.gpo.gov/cfr_2007/octqtr/45cfr164.312.htm).

FORRESTER®

Making Leaders Successful Every Day

Headquarters

Forrester Research, Inc.
60 Acorn Park Drive
Cambridge, MA 02140 USA
Tel: +1 617.613.6000
Fax: +1 617.613.5000
Email: forrester@forrester.com
Nasdaq symbol: FORR
www.forrester.com

Research and Sales Offices

Forrester has research centers and sales offices in more than 27 cities internationally, including Amsterdam, Netherlands; Beijing, China; Cambridge, Mass.; Dallas, Texas; Dubai, United Arab Emirates; Frankfurt, Germany; London, UK; New Delhi, India; San Francisco, Calif.; Sydney, Australia; Tel Aviv, Israel; and Toronto, Canada.

For the location of the Forrester office nearest you, please visit: www.forrester.com/locations.

For information on hard-copy or electronic reprints, please contact Client Support at +1 866.367.7378, +1 617.613.5730, or clientsupport@forrester.com.
We offer quantity discounts and special pricing for academic and nonprofit institutions.

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, customer insight, consulting, events, and peer-to-peer executive programs. For more than 28 years, Forrester has been making IT, marketing, and technology industry leaders successful every day. For more information, visit www.forrester.com.

FORRESTER®