

WHITE PAPER

Effective Information Security: A Win-Win Proposition for the Enterprise and IT

Sponsored by: CA

Christian A. Christiansen Gerry Pintal
September 2009

IDC OPINION

Driven by an accelerated increase in identity theft, consumer fraud, and other personal information-related thefts, industry groups and federal and state governments have taken aggressive steps to hold companies and their management accountable for confidential information disclosures. Similarly, enterprises are facing significant challenges in preventing the theft or accidental disclosure of intellectual property (IP) and corporate trade secrets. Ultimately, the challenge of establishing and implementing effective personal information and IP protection solutions falls upon the shoulders of IT management and staff.

Securing personally identifiable information (PII) and IP has become a high priority for enterprise management and IT. (See Appendix for additional definitions.) There are many disparate solutions for handling this problem. However, the problem itself is also "disparate."

IDC believes that an integrated, modular, and extensible approach, where the "disparate" solutions work together via business processes, is the future of information security. Connecting identities to roles and roles to access rights enables a continuous provisioning process. As an employee changes departments, his or her identity remains the same, but role and permissions change. For example, an employee move from payroll to sales may (or should) kick off processes on the employee's desktop that scan for unauthorized information that may have been left over from the employee's previous role (in payroll). Moreover, another process should be initiated that removes privileges associated with payroll processes but grants access to sales databases and tools. These business processes ensure that the employee does not retain inappropriate privileges, quickly gets the resources to do the new job, avoids separation of duties (e.g., book a sale and approve his or her own commission check), and eliminates associated audit problems.

IDC believes that CA's Information Security Suite produces enhanced data protection while increasing administrative efficiency by seamlessly integrating identity lifecycle management into its data loss prevention (DLP) solution. CA also integrates role and compliance management and log management into its solution. The CA approach provides IT with a "content-aware" IAM solution that establishes access rights based on identity and roles to guard against any purposeful or accidental disclosure of sensitive enterprise information and assists the enterprise in keeping up with and remaining in compliance with existing and future privacy regulations.

METHODOLOGY

IDC wrote this paper in August 2009. Its premises and opinions are based on leveraging a combination of research sources including IDC primary research on DLP, historical and current research through IDC customer and vendor surveys, monitoring of data and information losses reported in the press, and tracking of federal and state information security mandates and established industry data protection standards and best practices. In addition, IDC participated in briefings held by CA to gain an in-depth understanding of CA's Information Security Suite and DLP product and business proposition.

IN THIS WHITE PAPER

In this white paper IDC provides an overview of information security and its impact on enterprises, discusses IT operation challenges, and describes CA's answer to helping enterprise IT organizations attain increased visibility into and protection of their private and confidential data.

SITUATION OVERVIEW

A Brief History of Information Security

Not so long ago, IT's principal security focus was directed at preventing:

- Infrastructure security breaches
- Malware attacks from spreading throughout the enterprise
- Significant volumes of spam from consuming bandwidth and storage

Dealing with these issues increased enterprise investments in security-related technologies. It also made enterprise network infrastructures more complex and added to IT's already demanding workload.

Recognizing Street Value of Enterprise Data and Information

In the past several years there has been a major shift in the motivational drive behind attempts to breach established enterprise security infrastructures. The new enterprise security risk factor is "for profit" gain by stealing enterprise data. A crime ecosystem comprising cybercriminals, cybergangs, and organized crime has recognized the significant value of confidential data stored and maintained by enterprises. These criminals have partnered with highly skilled cyberdevelopers to innovate and develop new and creative methods for breaching IT security specifically aimed at "stealing" proprietary data.

With frequent and regular press reports of company data losses and consequences that negatively impact customers, company reputations, and overall business performance, enterprise executives, senior managers, and IT recognize the serious risks and consequences posed by events leading to enterprise data leaks.

Corporate Data Losses: Infrastructure Security Is Not Enough

It is now well understood that data losses represent significant risks to an enterprise. Data losses can occur as a result of an external breach or as a result of inadvertent or malicious employee actions. Protecting the enterprise infrastructure from outside attacks is no longer sufficient.

One solution is to consider a business process that:

- Highlights violations of compliance with established policies
- Identifies the individuals involved
- Generates meaningful reports for all departments (IT, legal, HR, and management)
- Initiates a workflow document that coordinates a response to the incident
- Engages controls to prevent further violations

While many enterprises already have established manual processes to accomplish these functions, a semiautomated business process that works across different technologies and corporate organizations can provide a faster response to help mitigate incidents and reduce or eliminate their repetition.

Virtually all corporate data is created and maintained in digital form. Network infrastructures, computers, and their associated peripheral technologies create a dynamic high-speed environment for processing, flow, and storage of data that makes it increasingly more difficult and time consuming for IT to effectively protect against outside attacks and the purposeful or accidental misuse of data by employees. Without effective tools to assist IT with DLP, the risk of a meaningful data loss occurrence is significant.

Personal Identification Information, Corporate Data, and Intellectual Property

Data: Life Blood of the Enterprise

Data is the life blood of every business, large and small. For the purposes of this paper, we focus on the types of data that are considered to be proprietary, confidential, or private and that if released, lost, or stolen could result in severe consequences for the enterprise and others affected. Data types are generally categorized as:

- Personally identifiable information (PII):** Information that can specifically identify an individual
- Intellectual property (IP):** Data that includes inventions (patents), trademarks, industrial designs, etc.

- ☒ **Nonpublic personal information (NPPI):** Information about a company that is not known by the public and if leaked could have a material impact on that company's stock value

These three data categories can also be thought of as existing in any one or all of three states: data at rest (DAR), data in motion (DIM), and data in use (DIU).

Employee Actions: Business Risks

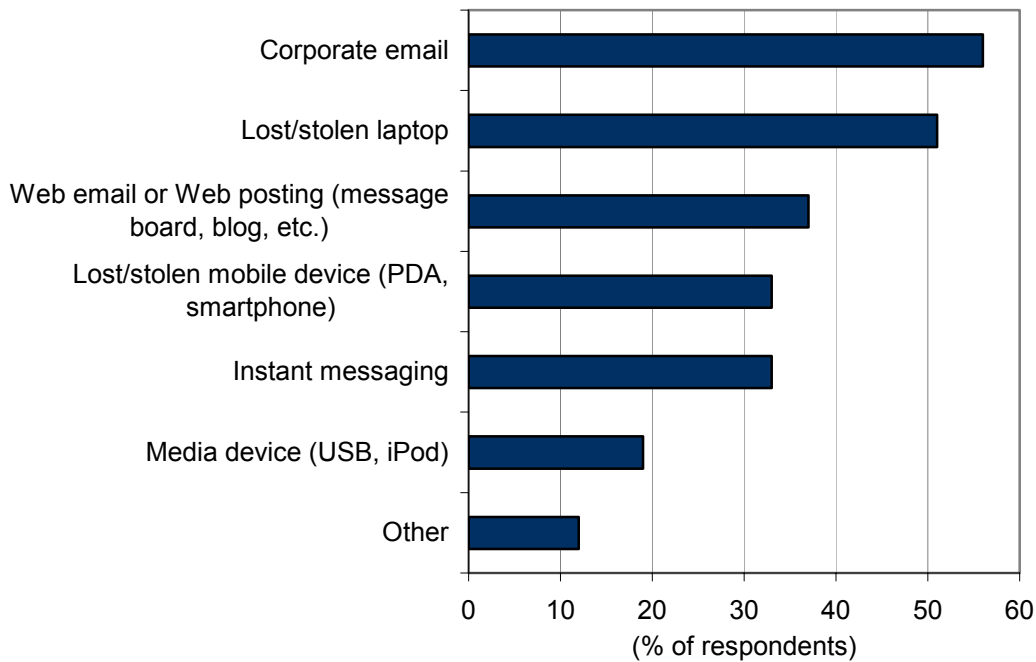
Many, if not all, employees have access to communication-oriented applications such as email, Web access, and instant messaging (IM) to perform their day-to-day business activities. Although these applications represent "leakage" points, they also represent avenues for employees conducting inappropriate activities that can place a business at risk.

In a 2008 IDC survey on DLP, participants who had experienced data losses within the past 18 months were asked how the data losses had occurred. More than half (56%) of the respondents reported confidential data losses through their corporate email systems. Figure 1 provides a snapshot of the various avenues of data losses experienced by survey participants.

FIGURE 1

Sources of Data Loss

Q. How did the leak(s) of confidential information occur?



Source: IDC, 2008

Data Loss Statistics and Costs

According to the Privacy Rights Clearinghouse, nearly 245 million electronic records have been breached since January 2005, and according to U.S. government estimates, enterprise data loss cost businesses nearly \$105 billion in 2008.

Government Mandates and Industry Standards

With rising incidents of identity theft and data breaches occurring worldwide, the U.S. government and many individual states have enacted data privacy laws that require businesses and organizations to notify customers in the event that their PII is lost, stolen, or leaked. The potential impact on businesses for noncompliance with these laws and mandates could be severe. The risks of noncompliance are as follows:

- ☒ **GLBA.** Noncompliance with GLBA can result in civil penalties of up to \$100,000 for each violation. Officers and directors of financial institutions are personally liable for civil penalties of up to \$10,000 for each violation and serve up to five years imprisonment for each violation.
- ☒ **HIPAA.** Noncompliance with HIPAA carries fines. The fine for a simple violation such as not documenting release of PHI for every client is \$100 per violation per client per year. The maximum fine per standard violation is \$25,000 per year. For misuse of patient data, the fine could be \$250,000 plus jail time for executives.
- ☒ **SOX.** Noncompliance with SOX carries fines of up to \$500,000 with the potential of prison time for company executives.
- ☒ **PCI.** Noncompliant PCI companies risk losing their ability to process credit card payments and risk being audited and/or fined.

In addition to the aforementioned regulations, many states have enacted data privacy laws requiring certain security procedures to be in place in order to conduct business in their jurisdictions and that businesses and organizations notify individual customers and members in the event that their PII is lost, stolen, or inadvertently released.

Information Security Suites

Senior management often pressures IT organizations for continued improvement in policy compliance. However, IT may not be fully aware of current regulatory and policy requirements and constraints. Many existing information security solutions, currently managed by IT, do not provide the breadth of features and functions required to effectively address the broad scope of information security and policy issues. The net result of implementing limited information security solutions is that they represent more work for IT, are unable to effectively respond to constantly changing policies and environments, and are piecemeal approaches that do not address the "stove piped" way businesses store and maintain data. Many approaches are difficult to integrate into existing enterprise infrastructure environments, are narrow in scope, and do not take into consideration the IT resources required to support employee provisioning and deprovisioning.

Solution Options: Advanced Information Security Suites

Facing government and industry regulations with the potential for costly fines, risks of damage to brand, impact on market valuation, and the threat of intellectual property losses, enterprise management and IT professionals are in need of and are seeking advanced integrated data security solutions to assist them in protecting their businesses against the potentially significant consequences of data loss events.

Data security is a key to surviving audits (internal and external) and avoiding costly privacy breaches. Once it is known, through alerts or audit anomalies, that a likely sensitive data breach has occurred, IT management in collaboration with HR and compliance officers can monitor potential misuse (inadvertent and deliberate) and take appropriate steps to mitigate against potential losses.

Information security solutions that require a significant investment in staff time to evaluate, test, deploy, configure, and maintain while failing to address core data protection issues leave the enterprise vulnerable to data disclosures. An advanced data security suite must be extensible and capable of delivering comprehensive protection against data losses and at the same time delivering on minimizing IT workload and ultimately producing a rapid time to value.

IDC believes that an effective and comprehensive information security suite provides the following:

- ☒ **Comprehensive data discovery.** Without a comprehensive data discovery capability, corporations will find it difficult to accurately locate and identify their "sensitive" data. A DLP solution must be able to automatically detect the presence of such data on desktops, laptops, and removable storage devices. IDC believes that a comprehensive DLP solution must provide global protection for all DAR, DIU, and DIM.
- ☒ **Continuous data monitoring.** Because there is continual churn in the creation, elimination, and location of sensitive data, data monitoring needs to be a continual process. Continuous monitoring of sensitive data provides a timely and accurate view of data migration, interactions, and transactions. Continuous monitoring is an important security feature that provides alerts when sensitive data is being "harvested" from applications or databases. With dynamic monitoring, inappropriate access to sensitive data in applications and databases can be detected quickly in order to prevent the data from being transferred to removable media or transmitted to inappropriate parties via communication vehicles such as email.
- ☒ **Flexible enforcement and control.** Because policies are dynamic and often contentious issues, particularly if they appear to impede staff productivity, enforcement flexibility is needed. Enforcement options must range from casual warnings to strict prevention. Warning users in real time with alerts that they are about to violate corporate security policy can significantly reduce accidental data misuse or loss. Alerts and warnings must be understandable by both IT and non-IT personnel. In some cases, users may be allowed to violate policy, but logs must be kept and made available for further analysis and investigation. In other cases, the activity may be blocked, an explanation offered, and the activity escalated for further review and discussion.

- ☒ **Peripheral device monitoring and control.** While internal data control of company-owned and company-managed systems is important, control over employee-owned peripheral devices (especially USB flash drives and other such storage devices) is important because they have become critical "leakage" points. In addition, data must be controlled beyond corporate boundaries to partner organizations that have authorized access to sensitive data. This requires control capabilities that are network, operating system, and application independent.

- ☒ **Logging and log analysis.** Over time, logging features provide an accounting of events that can be analyzed for trends. Log analysis tools can:
 - ☐ Separate inadvertent violations from malicious activities

 - ☐ Provide guidance as to the extent and severity of potential misuse and breaches

 - ☐ Highlight the need for policy modifications or new policies

- ☒ **Reporting.** Reporting tools not only must be available to IT but also must generate reports that are usable, understandable, and relevant to IT, senior management, compliance officers, HR, corporate legal staff, and internal audit groups. With a mutual understanding of log data by all groups, policy creation and update processes will become more effective.

In addition to the previously mentioned data security suite features, IDC believes that the following complementary features should be considered as part of an overall information security solution:

- ☐ **Encryption and key management.** Policy-based encryption with centralized key management and recovery may be a requirement for certain information storage, shared access, and exchange.

- ☐ **Dealing with aged data.** As data ages, it becomes less valuable to the corporation, but it becomes more vulnerable to breaches and leakage. Some industry policies (i.e., PCI) and European privacy regulations may require that data be destroyed in a timely and comprehensive basis. An adaptable policy monitoring and enforcement capability will assist IT in dealing with these issues.

Future Outlook

Compliance with government mandates and industry standards continues to drive DLP purchases. DLP revenue is expected to reach \$1.2 billion by 2013. IDC projects the DLP market will continue to increase at a 34% CAGR through 2013.

CA OVERVIEW

CA Company Profile

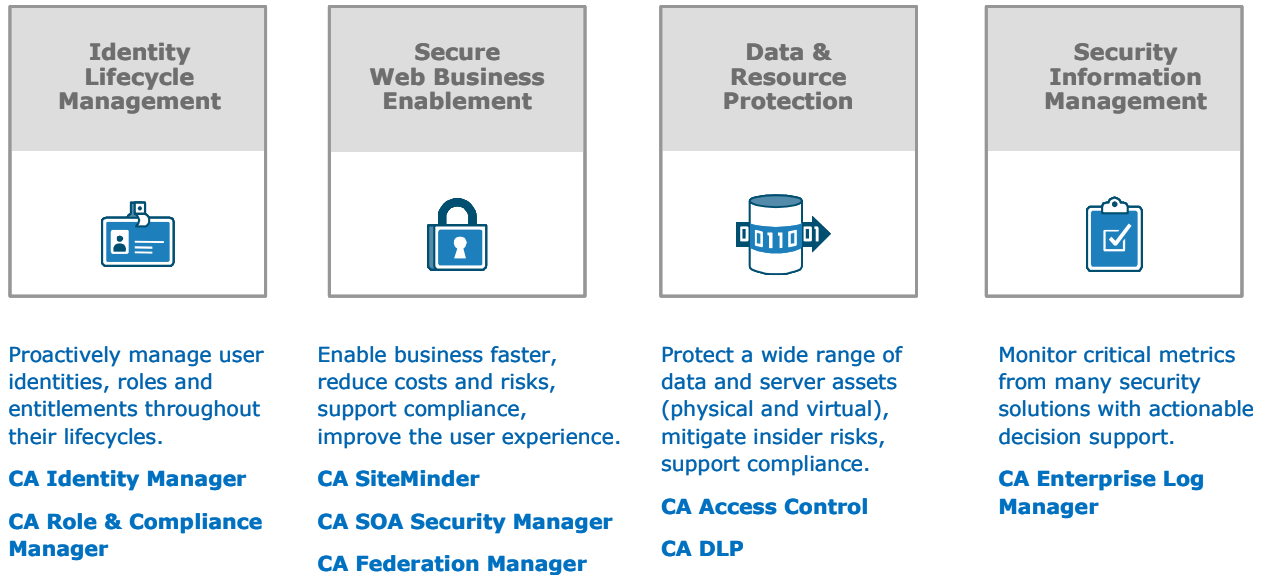
With global headquarters in Islandia, New York, CA provides IT management software worldwide. Founded in 1974, the company employs more than 14,000 people and offers hundreds of software products in its portfolio. CA has been a leader in the identity and access management market since 2003. CA products are available on a wide range of platforms and operating systems, from PCs to Unix to mainframes. The company also provides customer technical support and professional services, including consulting and education.

CA's Comprehensive Information Security System

Figure 2 provides a graphical view of the security functions provided by CA's Information Security System.

FIGURE 2

CA Information Security System



Source: CA, 2009

CA Identity Lifecycle Management

CA's Identity Lifecycle Management products provide complete management of employees, users, and customers from initial provisioning to deprovisioning. CA's Identity Manager and Role & Compliance Manager products function together to provide the following critical business functions:

- ☒ **Role Management** establishes a specific role model that fits the organization, defines what roles exist in the enterprise, and supports ongoing analysis and maintenance of roles as the business evolves.
- ☒ **Identity Management** assigns users to organizational roles, applies role-based user controls, provisions users with approved accounts and privileges, facilitates change requests and approvals over time, and offers user self-service for password and registration management.
- ☒ **Role and Compliance Management** certifies user roles and entitlements, performs real-time identity policy checks, detects security violations relating to specified segregation of duties, and provides dashboard views and compliance reporting.

CA Data & Resource Protection

CA's Data & Resource Protection (DRP) products provide a comprehensive approach to protecting an enterprise's sensitive data. DRP discovers and classifies all types of information to enforce security policies, provides protection against inappropriate server access and data losses, manages data access to established policies, simplifies the management and auditing of data and server access policies, and reduces overall data and resource protection costs. DRP features also include:

- ☒ **Data Loss Prevention** discovers and protects data at rest (stored data), controls data in motion (email, Web, etc.), controls data in use (saving, printing etc.), and supervises and reviews data (review, tag, etc.).
- ☒ **Privileged User Management** defines fine-grained access control, manages access with policies, leverages secure policy-based reporting, and protects against host data losses.

CA Security Information Management

CA's Security Information Management (SIM) application provides IT with enterprisewide visibility into and awareness of information security. CA SIM features include:

- ☒ **Enterprise Log Management** captures and collects log data, aggregates and analyzes log data, facilitates visualizing compliance and security postures, and provides proof of compliance for internal and external audits.

Secure Web Business Enablement

CA's Secure Web Business Enablement centrally secures access to Web applications and services while enhancing user experience through improved navigation and personalization. Capabilities and features include:

- ☒ **CA SiteMinder** is a centralized Web access management system that enables user authentication, single sign-on, authentication management, policy-based authorization, identity federation, and auditing of access to Web applications and portals.
- ☒ **CA SOA Security Manager** is a service-oriented architecture/Web services security software product that secures access to services by inspecting the security information contained in XML documents submitted by service consumers. CA SOA Security manager offers a centralized, policy-based authorization service, flexible authentication services, XML threat prevention, synchronized session management, identity federation, and standards conformance with standards such as WS-Security and integration with CA SiteMinder.
- ☒ **CA Federation Manager** is designed to ease the deployment of federated partnerships. It provides federation-focused administration, flexible deployment either as a standalone or as a complement to CA's SiteMinder Web Access Manager and integration options for multiple service provider and identity provider scenarios.

Real-World User Scenarios

To help organizations understand the significant information security value delivered by the CA Information Security System, the following scenarios illustrate how enterprises are vulnerable to accidental and malicious data losses and breaches without a comprehensive and effective information security system in place.

User Scenario 1: Disgruntled Scientist

A trusted DuPont employee, who had been employed for 10 years at the company's facility in Wilmington, Delaware, was offered a position in Taiwan but had to decline the offer because of personal reasons. Upon refusing the transfer, he was demoted and reassigned to DuPont's Ohio facility. Shortly after refusing the DuPont job in Taiwan, the employee interviewed for a position with a DuPont competitor. During that time, it is estimated that the employee downloaded some 22,000 abstracts and 16,000 technical documents from the company's in-house electronic library, **15 times** as many as the next highest user.

After noticing these unusually high data access rates, DuPont notified the FBI and Department of Commerce about his activities. Through subsequent investigations by the FBI, it is estimated that the employee had stolen more than \$400 million in trade secrets and was intending to provide them to his new employer. The former DuPont employee was subsequently tried and sentenced to 18 months in prison, having pleaded guilty to thefts of trade secrets.

In this scenario, we see that a comprehensive information security system, such as CA's Information Security Suite with content-aware IAM and supported by strong and effective policies, could have restricted the employee's unfettered access to proprietary data. If access were achieved, the system would have provided specific identity-based alerts of an information policy breach taking place. Establishing a policy that allowed IP such as patent applications and other technical data only to be stored in securely protected repositories and not to be saved on removable media or transmitted out of the enterprise regardless of the end user's identity or role would have provided a higher level of protection for the enterprise. Further, the DLP solution could have periodically searched enterprise servers and workstations for these types of sensitive data and, if found outside of the designated repository, removed them with appropriate notifications. In addition, when an employee resigns, is suspected to have an intent to resign, or exhibits morale issues, an established DLP "intent to resign" policy would trigger, placing the employee on heightened alert. DLP would then provide immediate alerts to IT and management of any subsequent download of trade secret documents.

User Scenario 2: Extortion and Potential Exposure of Patient Records

Although recent PII extortion attempts have drawn much attention, documented instances go back many years. In 2004, the University of California, San Francisco Medical Center (UCSFMC) received an email from a Pakistani woman, threatening exposure of patient information. The demand for payment included patient records as confirmed by UCSFMC and detailed in an investigative San Francisco Chronicle article pointing out the dangers of losing control of outsourcers and contractors.

The Medical Center had transcribed patient records to a California firm that outsourced to a Florida company, that outsourced to a Texas company, that in turn outsourced to a Pakistani firm. A Pakistani woman, who had failed to receive payment for her work, subsequently emailed the Medical Center threatening to publicly expose Medical Center patient records. Amazingly, all she wanted was \$500. She was paid and had promised to destroy the patient records. However, this is only the beginning of the story.

Subsequently, the Medical Center revealed the breach and began an investigation of the new and stricter privacy legislation (HITECH Act) that was included in a portion of the recent economic stimulus bill. The legislation amends and strengthens HIPAA privacy and security regulations. As a consequence of the HITECH mandates, the Medical Center was burdened with much stricter security policies that had to be developed and enforced.

Still, the question remains as to whether the medical records were destroyed. Given that simply "deleting" files is not enough to erase data from most PC disk drives,

security professionals still wonder if this data was ultimately exposed by the Pakistani woman or other contractors.

As for possible solutions, IDC believes that several are applicable to past and current problems. Central storage of the data with fully authenticated and authorized access by carefully vetting contractors could limit data movement to unauthorized firms and personnel. Background checks of these firms and their personnel should be a contractual obligation. Logging of all access requests and regular reconciliation against authorization privileges would indicate violations.

Data loss prevention, monitoring, and controls based on identity and role information provide IT with an added protective dimension by providing control of and a view into what information is being accessed and by whom. For example, with the CA solution, contractors and other nonauthorized individuals would be prevented from unauthorized file transfers, inclusion of patient data in emails, downloads to portable storage devices, and other prohibited activities on the basis of their identity. Prompt deprovisioning of access could prevent out-of-contract firms from accessing patient data. Security incident and event management could aggregate and analyze events from multiple systems to identify possible attacks on the patient data or even attacks against key contractors.

CHALLENGES/OPPORTUNITIES

CA's opportunity is to gain a solid leadership position in information security and information security management by tying in identity and roles to DLP, providing IT with relief from their already burdened workload. With CA's DLP solution, IT is able to push self-remediation opportunities out to end users while also allowing commissioned non-IT staff to perform provisioning and deprovisioning tasks. These added features clearly establish a win-win situation for IT and the enterprise.

The present and most challenging hurdle to CA's success in this competitive market is largely driven by the current world economic downturn. Although recent surveys have shown that security-related investments by enterprises are projected to be slightly higher or flat in the current economic conditions, budgets remain under tight control and security investments are being cautiously managed.

With respect to CA specifically, DLP and Active Directory integration are already done. However, the full solution, as described, requires tighter integration across CA's suite of solutions.

For CA, the next step is programmatic implementation so as to reduce services (e.g., system integration), move beyond its ability to generate reports for non-IT personnel (e.g., audit, legal, compliance, HR, and senior management), and push security out to non-IT people as business services. CA must deliver on the promises it has shown in demonstrations where business users initiate their own reports, create their own policies, and create their own compliance metrics.

Today, each CA product generates business-centric reports for consumption by HR and other non-IT staff. IDC would like to see CA take the next step, enabling non-IT people to generate reports for use by other non-IT people. In other words, IT does not

have to generate reports for auditors, HR, legal, senior management, and compliance officers because users can do it themselves with confidentiality and integrity and without violating their access privileges.

CONCLUSION

CA's comprehensive approach to enterprise information security raises the technological bar by providing IT with an effective, scalable, cost-effective solution that is based in the roles and identity of users. CA's solution provides IT with the security monitoring, reporting, and analysis tools to detect, understand, and respond to blatant or suspicious information security–related behavior.

With CA's complete "content-aware" IAM solution, enterprises gain a significant edge in preventing data losses from either external breaches or due to internal errors and/or malicious motives that can lead to costly fines, damage to reputation or brand, and loss of intellectual property. At the same time, CA's solution provides an effective way to simplify reporting for both internal and external mandatory audits.

APPENDIX

Government Laws and Mandates

GLBA

In 1999 the U.S. Congress enacted the Gramm-Leach-Bliley Financial Modernization Act (GLBA). GLBA mandates that financial institutions have an obligation to protect the security and confidentiality of their customers' NPPI.

HIPAA

In 1996 the U.S. Congress enacted the Health Insurance Portability and Accountability Act (HIPAA). HIPAA's privacy rule came into effect in 2003 and establishes regulations for the use and disclosure of individual protected health information (PHI).

SOX

In 2002 the Sarbanes-Oxley Act (Sarbox or SOX), also known as the Public Company Accounting Reform and Investor Protection Act of 2002, became a U.S. federal law.

PCI

The Payment Card Industry Data Security Standard is a worldwide information security standard assembled by the Payment Card Industry Security Standards Council (PCI SSC). The standard applies to all organizations that hold, process, or pass cardholder information from any card branded with the logo of one of the card brands.

Definitions

DAR: Data at rest; data residing on computers, corporate servers, or network shares at endpoints of the network

- ☒ **DLP:** Data loss prevention
- ☒ **DIM:** Data in motion; data moving through the network and leaving various exit points (Data in motion can be found in email, instant messaging, FTP downloads, printed data, or other data transfer methods exiting the network to known and unknown points.)
- ☒ **DIU:** Data in use; information on computer systems that is being viewed, analyzed, or worked on
- ☒ **DRP:** Data and resource protection
- ☒ **GLBA:** Gramm-Leach-Bliley Financial Modernization Act
- ☒ **HIPAA:** Health Insurance Portability and Accountability Act
- ☒ **HITECH:** Health Information Technology for Economic and Clinical Health Act
- ☒ **IAM:** Identity and access management
- ☒ **IM:** Instant messaging
- ☒ **IP:** Intellectual property
- ☒ **NPPI:** Nonpublic personal information (e.g., Social Security numbers, credit card numbers, drivers' license numbers, contact information, addresses, and passwords)
- ☒ **PCI:** Payment Card Industry
- ☒ **PCI SSC:** Payment Card Industry Security Standards Council
- ☒ **PII:** Personally identifiable information
- ☒ **SIM:** Security information management
- ☒ **SOX:** Sarbanes-Oxley
- ☒ **USB:** Universal serial bus
- ☒ **Web:** World Wide Web

Copyright Notice

External Publication of IDC Information and Data — Any IDC information that is to be used in advertising, press releases, or promotional materials requires prior written approval from the appropriate IDC Vice President or Country Manager. A draft of the proposed document should accompany any such request. IDC reserves the right to deny approval of external usage for any reason.

Copyright 2009 IDC. Reproduction without written permission is completely forbidden.