

Security Information Lifecycle

Data Retention of Event Logs for Compliance

By Eric Ogren
Security Analyst, Enterprise Strategy Group

April 2006

Table of Contents

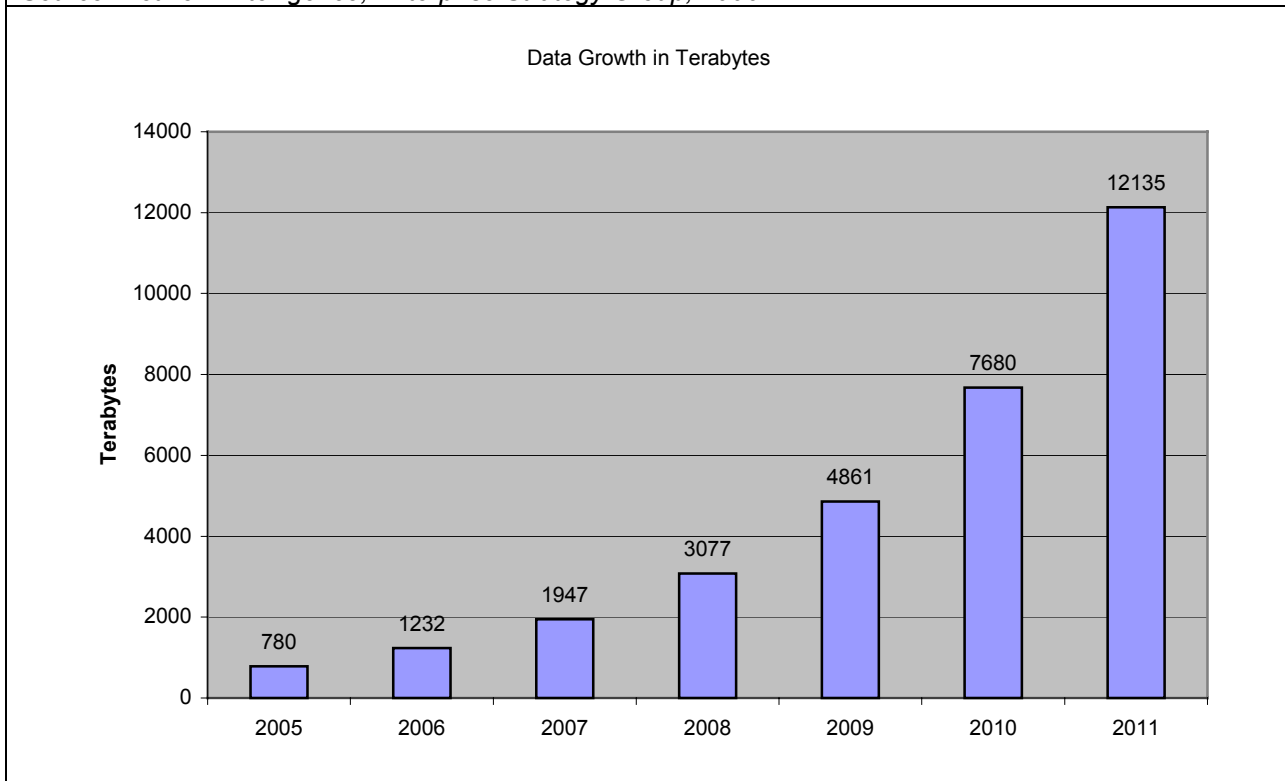
Executive Summary	2
Figure 1	2
The Compliance Climate	4
Figure 2	4
Network Intelligence and EMC Centra: Best Practices for Data Retention	7
Figure 3	7
Recommendations and Conclusions	9

Executive Summary

Government regulations mandate that information security abide by the proven best business practices of transaction logging, performance assessment, and rigorous auditing. For years, information security has bedeviled corporate IT as enterprises invested heavily in technologies such as firewalls, intrusion detection, and anti-virus software with little visibility and control as to how effective those investments were to the business. Regulatory compliance now makes it imperative that corporations not only secure sensitive information, but also be able to articulate how they manage the effectiveness of their security program over the complete lifecycle of their security information. Enterprise security teams are turning to Security Information and Event Management, SIEM, products to cost effectively automate the compliance reporting of security transactions and to work closely with storage vendors to keep security information secure for the duration of its data retention period.

Satisfying the reporting demands of government regulations and corporate security policies requires the retention of vast amounts of security data. Not only must the enterprise collect log and event data from high performance security products including firewalls and identity management systems, but auditors must also be able to go back several years to trace security violations. Compliance-driven data retention requirements are generating an explosion of security information, as shown in Figure 1.

Figure 1
Data Retention Regulations Lead to Explosion in Stored Security Information
Source: Network Intelligence, Enterprise Strategy Group, 2006



The chart is based on Network Intelligence experiences for a typically active Fortune 500 corporation generating 250,000 events per second, which required 780 terabytes of storage in 2005. Growth rates are based on ESG research showing a 58% CAGR for all corporate archived data. These estimates may grow as requirements expand to include additional security solutions and inclusion of application log data.

Enterprises tailor Information Lifecycle Management principles to the data retention requirements of security data, what ESG refers to as the Security Information Lifecycle (SIL). One key differentiator in the Security Information Lifecycle is the requirement to act on analysis of correlated events while those events are written to persistent storage. SIL requirements include the efficient collection of security information and events, processing for security policy violations, cost-effective high performance secure retention of information, and access to stored data by auditors for compliance reporting. Two of the industry leaders, EMC Centera and Network Intelligence, have partnered to offer a strategy and solution for managing the entire Security Information Lifecycle for enterprises facing requirements for complying with government regulations over the next several years.

This special report, commissioned by EMC and Network Intelligence, examines a comprehensive approach to managing large volumes of log data for regulatory and internal security policy compliance. The purpose is to provide information and make recommendations for data retention best practices to assure true compliance. Information in this report derives from Enterprise Strategy Group research and interviews with security executives of global operations.

The Compliance Climate

Demonstrating compliance with government regulations, industry standards, and internal security policies dominates enterprise security priorities. Many organizations often have multiple regulations driving their compliance requirements. For instance, a large financial institution will likely have to comply with Sarbanes-Oxley (public company), GLBA (financial company), CA 1386 (California customers), PCI (credit card processing), Basel II (European risk management), and the local privacy regulations enacted in other countries of the world. In an international economy, US institutions must comply with non-US regulations and non-US corporations conducting business in America must comply with appropriate US regulations. Each of the regulations has distinct collection, analysis, and reporting requirements that must be factored into the security information lifecycle.

The major regulations that this special report covers include a range of federal government mandates, vertical industry regulations, international standards and specifications, and private industry consortia. There are common elements between these regulations, but all share the requirement to capture security information, to use this information to report on security operations, and to retain this information for an extended period of time, as shown in Figure 2. **One effect of government regulations is that security information, including event logs and transaction logs, has now become legal records that must be produced when requested by legal authorities.** This could potentially stretch data retention periods to the duration of the litigation process.

Figure 2
Data Retention Periods of Leading Regulations
Source: Enterprise Strategy Group, 2005

<i>Regulation</i>	<i>Data Retention Requirements</i>	<i>Penalties</i>
Sarbanes-Oxley	5 years	Fines to \$5M Imprisonment to 10 years
PCI	Corporate Policy	Fines Loss of credit card privileges
GLBA	6 years	Fines
Basel II	7 years	Fines
HIPAA	6 years 2 years after patient death	\$25,000
NERC	3 years	TBD
FISMA	3 years	Fines
NISPOM	6 months to 1 year	Fines

Each of these regulations, and their data retention references, are:

- **Sarbanes-Oxley Act of 2002 (SOX).** Public companies with annual revenues exceeding \$75 million must protect information affecting the organization’s financial reporting. Section 404

involves security management for disclosure, modification, or interference with systems operations with data retention requirements specified in 1520 (a)(1) Destruction of Corporate Audit Records. Specifically, “(a)(1) Any accountant who conducts an audit of an issuer of securities to which section 10A(a) of the Securities Exchange Act of 1934 (15 U.S.C. 78j-1(a)) applies, shall maintain all audit or review workpapers for a period of 5 years from the end of the fiscal period in which the audit or review was concluded.”

- **Payment Card Industry Data Security Standard (PCI).** PCI members, merchants, and service providers that store, process or transmit cardholder data must submit annual audit statements covering 12 sections of requirements. Additionally, these security requirements apply to all “system components” which is defined as any network component, server, or application included in, or connected to, the cardholder data environment. See Requirement 10, Track and monitor all access to network resources and cardholder data. Section 10.7 states, “Retain your audit trail history for a period that is consistent with its effective use, as well as legal regulations. An audit history usually covers a period of at least one year, with a minimum of 3 months available online.”
- **Gramm-Leach-Bliley Act of 1999 (GLBA).** Mandates that financial institutions secure the confidentiality of consumer financial information, and be able to attest that controls against threats and inadvertent disclosures are working. See GLBA 501 Interagency Guidelines Establishing Information Security Standards for data retention guidelines.
- **Basel II Capital Accord.** International banking regulation includes provisions for aligning capital reserves with levels of credit risk and operational risk. Reporting on the security profile of the financial institution is a significant factor of the Basel II accord. Best practices for data retention for Basel II can be found in the Federal Reserve Board Notice of Proposed Rulemaking, Section 22 Qualification Requirements.
- **Health Insurance Portability and Accountability Act (HIPAA).** Protects health information that matches a patient identity with health status data. HIPAA regulations coverage includes doctors and hospitals, pharmaceuticals, insurance companies, claims processors, and clinical research organizations. Sec 64 Fed. Reg. 59994 of the statute articulates data retention periods, citing specifically, “documents relating to uses and disclosures, authorization forms, business partner contracts, notices of your information practice, responses to a patient who wants to amend or correct their information, the patient’s statement of disagreement, and a complaint record must be maintained for 6 years.”
- **National Energy Commission (NERC).** The North American Electric Reliability Council sets guidelines and standards for electric utilities. NERC specifies cyber security data retention requirements in its Critical Infrastructure Protection standards, CIP-002-1 through CIP-009-1, section D1.3.2 Data Retention which states, “The compliance monitor shall keep audit records for three calendar years.”
- **Federal Information Systems Management Act (FISMA).** Government agencies must centrally manage and report on risks to the confidentiality, integrity, and availability of information and systems. FISMA guidelines for data retention are documented by the National Institute of Standards and Technology in the NIST 800-61 special publication titled “Computer Security Incident Handling Guide”. Section 3.4.3, Evidence Retention, clarifies the data retention requirement, “As discussed in Section 3.4.2, General Records Schedule (GRS) 24 specifies that incident handling records should be kept for three years.”
- **National Industrial Security Program Operating Manual (NISPOM).** All government agencies and contracting organizations must implement security processes to protect the confidentiality, integrity, and availability of classified data. NISPOM Section 8-602 (a)(4), Audit Record Retention requires, “Audit records shall be retained for at least one review cycle or as required by the Cognizant Security Agency.”

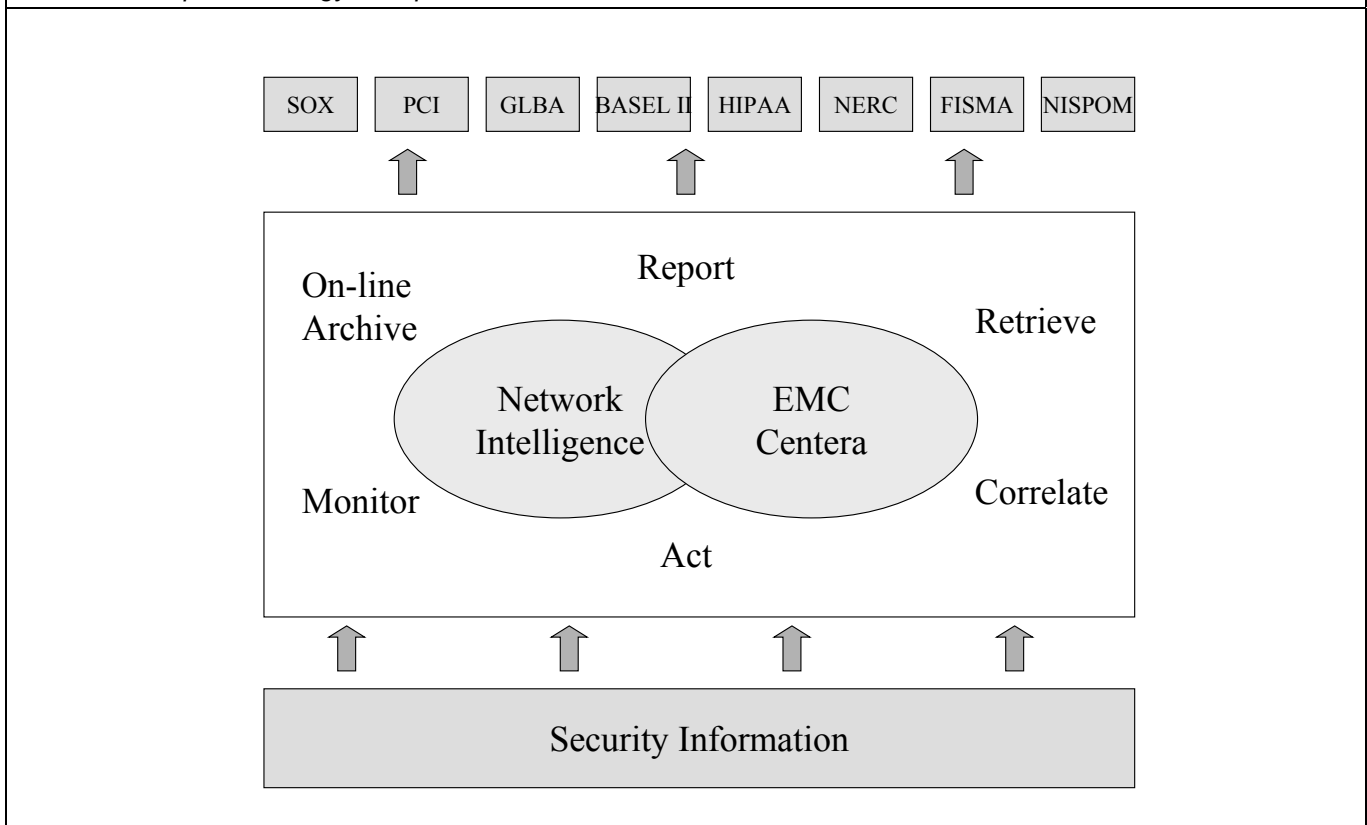
All of these regulations share requirements for managing the security information lifecycle. The specifics of compliance reporting vary per the interests of the regulation, the length of the security information lifecycle, and the penalties for non-compliance.

Penalties for non-compliance include monetary fines, civil liability and executive accountability. In some cases, such as with Sarbanes-Oxley, the statutes allow for fines that may reach into the millions of dollars. However, the largest penalties for non-compliance are likely to be the market-driven costs of having the company name associated with a security breach, and not being able to demonstrate reasonable security precautions with an acceptable compliance statement. The damaged trust relationship effects customer satisfaction, consumer confidence, and the organization's ability to compete in the marketplace. Recovering from such events could take years.

Network Intelligence and EMC Centera: Best Practices for Data Retention

To reduce the operating costs of compliance programs, enterprises must implement solutions that automate procedures across the security information lifecycle for multiple regulations. Solutions that integrate the best of SIEM with the best of on-line archival storage are proven to be cost-effective approaches for meeting enterprise security information lifecycle management requirements. Network Intelligence and EMC Centera solve the large problem of security data management for enterprises, as portrayed in Figure 3. The Security Information Lifecycle partners consolidate the technical implementation of complying with the demands of multiple regulations to give enterprises a high performance solution that will meet corporate compliance reporting needs for years.

Figure 3
Network Intelligence and EMC Centera Approach
Source: Enterprise Strategy Group, 2006



Network Intelligence brings security expertise to the partnership with EMC Centera. A leader in the SIEM market, Network Intelligence is now focused on the enterprise problem of managing the Security Information Lifecycle for compliance. Meanwhile, EMC's Centera product line leads the storage market with its ability to meet the long-term storage and access demands of information in its final and static form, such as security information represented by log files and event data in on-line archives. EMC Centera ensures that the SIL solution can scale as data requirements expand during

Enterprise Strategy Group

the life of the solution. The major benefits of an EMC Centera and Network Intelligence solution include:

Collect security information. Network Intelligence has built interfaces to collect security information from vendor products such as firewalls, intrusion detection, identity management, configuration scanning, and web servers. Enterprise requirements for security information will increase in the coming years, and Network Intelligence has proven expertise in integrating new security data into the SIL solution.

Deliver with high performance. Performance is everything in a network appliance. ESG experience finds that vendors with high performance have a sustaining advantage over competitors who face prohibitive costs of re-architecting for performance. Network Intelligence wisely avoids attempts at normalizing all security information before writing to storage. Streaming security information to storage, and tackling the formatting and analysis problems in the background, is a nice architectural decision to deliver the high performance necessary to satisfy heavy corporate requirements.

Customize reporting. Every organization needs to generate multiple sets of compliance reports from stored security information. Network Intelligence deploys canned reports to get the enterprise up and running, and offers tools that allow the enterprise to customize the solution to their specific needs. No two enterprises look alike, and this allows corporate IT generate compliance reports that are meaningful to the enterprise and actionable by operations teams.

Trust the content. EMC Centera implements the Content-Addressed Storage architecture to ensure that security information written to on-line archives is authenticated and cannot be modified. Using EMC Centera's Content Addressable Storage technology, classes of security information can be marked as un-erasable over a given retention period to comply with corporate and government data retention policies, or be put on litigation hold if ordered. Corporate auditors can be assured that the data retrieved from storage exactly matches what was securely written several years before.

Transparently manage information retention classes. Compliance regulations feature varying durations of information retention. EMC Centera allows administrators to easily declare and transparently enforce retention policies, access control restrictions, and audit rules. No security information can disappear without a trace, but data is easily removed from the storage structures when the compliance retention period expires.

Scale easily to meet future needs. Security information lifecycle solutions will steadily consume storage as the business grows and as regulations inevitably extend data retention requirements. EMC Centera has built in enterprise capability to cost-effectively expand capacity to petabytes of storage, automatically discover and reconfigure new drives, and transparently replicate storage for business continuity and disaster recovery protection.

The EMC Centera and Network Intelligence approach is a solution focused on the real-time needs of analyzing security information, quickly writing events to on-line archives, and efficiently retrieving information when required. This is delivered with an ease of administration and a low total cost of ownership that goes right to the enterprise compliance management bottom line.

Recommendations and Conclusions

Managing the entire security information lifecycle entails a collective commitment from security, application, and storage operations teams. This is not an activity that can be conducted in isolation by the information security group. Enterprises are transitioning compliance management from manual processes to automated procedures to natural best practices, where corporations would not consider running their business without managing the security information lifecycle. ESG recommends that enterprise IT plan for the long-term, and combine the benefits of Network Intelligence data gathering and reporting with the EMC Centera strengths of information lifecycle management in the storage system.

Plan for the explosion of security information. Reporting requirements for security information are going to increase. Regulations are sure to call for log data from additional solutions. Plan now for performance to handle streams of security information without impacting application performance and storage capacity that offers efficient growth paths as the enterprise storage requirements grow.

Architect storage processes for managing the entire Security Information Lifecycle. Corporations that are automating compliance procedures must look ahead several years to architect for the entire security information lifecycle. This includes procedures for assuring the authenticity of data in storage, archiving data to secondary storage, and security information deletion at the end of the lifecycle. Storage architectures should be as self-configuring and as self-correcting as possible.

Integrate security information and event management into mainstream storage management. Security is a fundamental capability intrinsic to all corporate operations. ESG recommends that enterprises integrate security information lifecycle management teams within storage operations. Security information should be treated with the same care as corporate applications and financial data.

Network Intelligence and EMC Centera stand out for their proactive approach to simplifying the enterprise task of managing the Security Information Lifecycle. Together their solution resolves two major challenges that enterprises face in meeting the data retention requirements to comply with government regulations – handling the explosion of fixed security information content and minimizing the cost and complexity of managing active archives of security information. ESG believes that EMC Centera and Network Intelligence bring unique synergies to the security information lifecycle that delivers long-term sustaining benefits to any enterprise.

All trademark names are property of their respective companies. Information contained in this publication has been obtained by sources The Enterprise Strategy Group (ESG) considers to be reliable but is not warranted by ESG. This publication may contain opinions of ESG, which are subject to change from time to time. This publication is copyrighted by The Enterprise Strategy Group, Inc. and was sponsored by Network Intelligence and EMC. Any reproduction or redistribution of this publication, in whole or in part, whether in hard-copy format, electronically, or otherwise to persons not authorized to receive it, without the express consent of the Enterprise Strategy Group, Inc., is in violation of U.S. Copyright law and will be subject to an action for civil damages and, if applicable, criminal prosecution. Should you have any questions, please contact ESG Client Relations at (508) 482.0188.