RSA®

The Security Division of EMC

White paper

# Log Management Best Practices

## The Foundation for Comprehensive Security Information and Event Management

# Executive Summary

Log (event) management is the collection, analysis (real-time or historical), storage and management of logs from a range of sources across the enterprise. It is the foundation for comprehensive security information and event management (SIEM). Organizations which develop best practices in log management will get timely analysis of their security profile for security operations, ensure that logs are kept in sufficient detail for the appropriate period of time to meet audit and compliance requirements, and have reliable evidence for use in investigations.

Businesses face a number of challenges that make best practices in log management an increasingly important part of an overall enterprise IT security strategy. These include the need to control the vast amounts of data being generated by more and more systems, the increased requirements of today's regulated environment and a new breed of more advanced attacks.

By establishing best practices in log management, information executives can bring tremendous value to their organization by avoiding costs and increasing efficiencies in areas such as compliance, risk management, legal, forensics, storage and operations. Best practices in log management should be based on the requirements of applicable regulations and standards, guidance from legal counsel, business and operational objectives, and risk analysis.

Although best practices should be developed by each individual organization based on their particular environment, there are some general best practices which can be universally applied. This paper is intended to help organizations develop their own comprehensive set of best practices by providing a set of 40 recommended best practices covering logging policies, procedures and technology; log generation and capture; log retention and storage; log analysis; and log security and protection.

## Contents

## Definition of Log (Event) Management

A log is a record of an event or activity occurring within an organization's systems or networks. Examples include a firewall allowing or denying access to a network resource, a change to the configuration of the operating system performed by an administrator, a system shut down or start up, a user logging-in to an application, or an application allowing or denying access to a file. For more examples of events or activities, please see appendix 1, "Sources and contents of logs." Log (event) management is the collection, analysis (real-time or historical), storage and management of logs from a range of sources across the enterprise including security systems, networking devices, operating systems, and applications.

Log management is the foundation for comprehensive security information and event management (SIEM) including the following use cases:

- Real-time threat detection and mitigation
- Incident investigation and forensics
- Compliance to regulations and standards
- Capacity planning, performance and uptime
- Evidence for legal and human resources cases
- Detecting and preventing IP theft
- Auditing and enforcing employee productivity
- Troubleshooting system and network problems
- Auditing and enforcing IT security policy

## Why do Logs Matter for Security and Compliance?

Without sufficient collection, regular review and long-term retention of logs, your organization will not be in compliance with regulations nor able to properly protect its information assets. Logs provide a way to monitor your systems and keep a record of security events, information access and user activities.

Today's regulated environment coupled with a new breed of more advanced attacks makes log management an increasingly important component of your IT security strategy. A log management capability will enable you to detect unauthorized activities in real-time and to ensure logged data is available for audits and investigations and properly stored over its entire lifecycle.

The inability to manage logs is one of the major reasons that enterprises fail compliance audits. For example, inadequate review of audit logs is one of the top five IT control weaknesses cited by Sarbanes-Oxley auditors. Inadequate logging is also one of the top three areas of failure for the Payment Card Industry (PCI) Data Security Standard (DSS) according to PCI auditors.

Lack of competency in log management is also a major reason for data compromises. For example, MasterCard's forensic research indicates that the lack of real-time security monitoring is one of the top five reasons that merchants are getting hacked. In their investigations of companies which have suffered data breaches, the US Federal Trade Commission (FTC) has found that one of the major causes was failure to use sufficient measures to detect unauthorized access.

Without adequate log management, it is very difficult for enterprises to investigate and recover from a security breach. Massive data breaches have been headline news over the last couple of years. In many cases, these companies did not retain sufficient logs extending back in time to the initial intrusions, making it nearly impossible to determine exactly how the attack took place.

Regulation has also stretched out required retention time frames. For example, to prove the integrity of financial reports, corporate governance regulations require audit records be kept for many years. To account for disclosures of personal information, privacy regulations create the need for years-long storage of access logs.

Organizations which develop best practices in log management will get timely analysis of their security profile for security operations, ensure that logs are kept in sufficient detail for the appropriate period of time to meet audit and compliance requirements, and have reliable evidence for use in investigations.

## Challenges Addressed by Log Management

Businesses face a number of challenges that make best practices in log management an essential part of an overall enterprise IT security strategy:

1. The huge number and variety of systems generating logs

Over the last few years, in response to increased security threats, organizations have deployed many security systems – including intrusion prevention, patch management and anti-virus systems. As more business processes have been automated, more network devices, servers, storage subsystems and applications have also been added to the environment. The result is an increasingly larger and complex mix of systems generating logs. See appendix 1, "Sources and contents of logs."

With so many sources of logs, it is very difficult to make sense of them. It is hard to determine the overall security profile or get a complete picture of information access and user activities. For example, auditors may be expected to read reams of print-outs from many different systems in order to piece together evidence that only authorized users are accessing protected information. These kinds of activities make audits very expensive.

Without sound retention policies, logs from so many varied sources will likely not be getting stored properly. Logs with little value from some sources may be getting stored while important records from other sources may not be stored at all.

### 2. The volume of logged data

Global 2000 organizations can generate in excess of 10 TB of raw logs each month or more. With this amount of data, it is no wonder that many companies that collect logs do not actually analyze them because it is too difficult. Even if procedures for reviewing the logs have been established, often they are not followed reliably because it is extremely tedious to go through so many logs manually. Businesses need to develop best practices for analysis and reporting in order to make use of this critical information. It is also important to determine retention / retrieval strategies that will enable auditors and investigators to easily sort through the mountains of data to get the information they need.

### 3. The changing threat landscape

The attacks perpetrated nowadays are not just disruptive attacks such as the I LOVE YOU virus or denial of service attacks but very targeted and sophisticated attacks carried out by organized crime against specific information assets over long periods of time. In a recent high profile case, a large retailer had their systems infiltrated undetected over a period of 18 months.

This kind of environment calls for effective real-time monitoring to better detect intrusions, and for detailed logging of information that will be relevant in the case of a security breach. The need to go back in time over a period of several months or even years to collect evidence is real. The length of time organizations need to retain logs must be aligned with this new reality. Log records must be complete and readily retrievable to be useful during an incident investigation.

### 4. The more stringent regulatory requirements

Over the past several years, there has been a flood of regulations and legislation globally, mandating the protection of information. Organizations now have a legal obligation to protect information and are required to prove that their security measures are adequate.

Logging serves two functions for compliance. Logging is a central pillar of any security program and therefore essential for protecting information. Logging can no longer be left disabled and/or logs left un-reviewed if the organization wants to meet its legal obligations to protect information.

Logs are also the essential evidence for proving compliance or conformance to policy. Without logs, it is very difficult to impossible to answer questions such as, "Has this financial data been changed without proper authorization?" or "Were there any unauthorized disclosures of this health data? or "Are accesses to cardholder data limited to those with a business need?"

In the new regulated environment, most organizations are subject to multiple regulations and periodic internal or independent audits of their information systems to determine the adequacy of security measures. Logs must be collected in sufficient detail to enable an assessment and be readily available for review by the auditor.

Once an audit is completed, the organization will likely need to retain certain logs, often for years, in case the logs are requested as evidence by the regulators or the courts. Log retention requirements are now driven by the need to have the right information on hand to meet audit cycles and then retained long-term to meet the legal requirements for record keeping.

### 5. The increasing number of stakeholders

It is no longer just security and network operations that require information from logged data. Other groups across the enterprise need this information including Human Resources, Legal, Internal Audit, Finance, Engineering, Customer Service, Sales and Marketing. For example, HR needs it for managing personnel issues to prove employee behavior. Legal, Internal Audit and Finance use the information in compliance initiatives. Logs can help groups across the enterprise monitor employee productivity and track access to intellectual property. Best practices in log management should provide stakeholders across the organization with secure, quick and reliable access to the information they need.

### 6. The uncertainties of future regulatory and legal issues

There are more regulations in the pipeline worldwide. For example, comprehensive privacy legislation in the US is under discussion, and other geographies such as India and China are looking into introducing new laws. With future regulations, it is impossible to determine what logs will be necessary to prove compliance. Litigation due to security and privacy breaches has already begun. In fact, it is

predicted that security and privacy breaches will create the next significant wave of class action law suits. If an organization faces a lawsuit because of a breach, it may need to produce evidence of information access.

Another trend creating uncertainty is the increasing number of business partner agreements with specific provisions around information security including the right to audit. It is difficult to know what kind of logs a business partner may require down the road during a security audit. Organizations need to develop best practices in log management that can plan for these uncertainties with respect to what logs will be required when.

## The Business Value of Best Practices in Log Management

Most organizations have not yet developed and implemented best practices in log management however, because this capability is becoming so important, it is reaching the top of the agenda for many CIOs and CISOs. According to a recent study by TheInfoPro industry analyst group, security information and event management has become one of the top five information security projects for Fortune 1000 companies.

By establishing best practices in log management, information executives can bring tremendous value to their organization in these areas:

### Compliance

- Sufficient collection and retention of logs can help avoid the costs of non-compliance such as fines
- Reduces on-going audit costs by reducing the time it takes to complete an audit
  - Have the right log data and reports readily available for auditors
  - Be able to quickly prove requirements are met

### Risk Management

- On-going review and real-time monitoring of logs can help detect or prevent unauthorized access and reduce the risk of security breach
  - Protects brand, relationship with customers, and reputation
  - Avoids notification and legal cost
  - Avoids fines and litigation costs

### Legal

- More complete logs and efficient evidence collection reduces legal costs
  - Have evidence for a wrongful dismissal case such as user activity logs
  - Have evidence for a privacy case such as information disclosure logs
  - Have evidence for an intellectual property theft case such as software development access logs

### Forensics

- In the event of a breach, having quick access to the right logs will save money by making evidence collection easier and faster
- Makes finding the cause and implementing remediation easier and faster
- Helps stop attacks before they escalate, saving money
- Makes system recovery and damage clean-up after breach easier and faster
- Increases the chances of catching the culprits

### Storage

- Storing the right logs for appropriate length of time and enabling ready retrieval reduces costs
- Can assist with information classification
- Uses the most cost-effective storage based on the need for the information

### Operations

- More effective log analysis reduces monitoring costs such as personnel costs
  - Frees up personnel to do more productive tasks
- More effective monitoring reduces downtime and increases efficiencies by focusing on the right threats (reducing false positives)

## Inputs Into Your Organization's Best Practices

Best practices should be based on the requirements of applicable regulations and standards, guidance from legal counsel, business and operational objectives, and a risk analysis.

1. Requirements of regulations and standards

There are many regulations and industry standards mandating the protection of information such as:

- Sarbanes-Oxley (SOX)
- Health Insurance Portability and Accountability Act (HIPAA)
- Gramm-Leach-Bliley Act (GLBA)
- Federal Information Security Management Act (FISMA)
- Global privacy regulations[1]
- State breach notification laws (e.g. SB 1386)[2]
- Food and Drug Administration's 21 CFR Part 11 (Part 11)[3]
- Payment Card Industry (PCI) Data Security Standard (DSS)
- North American Electric Reliability Council (NERC) Cyber Security Standards

Most of regulations do not provide specific requirements; instead they expect organizations to implement "reasonable and appropriate measures" to protect information guided by the requirements of information security standards such as:

- Control Objectives for Information Technology (COBIT)
- National Institute of Science and Technology Special Publications 800 Series (NIST SP 800)
- Federal Financial Institutions Examination Council IT Handbook on Information Security (FFIEC)
- International Standards Organization "Code of Practice for Information Security Management" (ISO 17799/27001)

For specific compliance requirements regarding log management, organizations will need to go beyond the information provided in the regulations themselves and also consult the relevant information security standards. For more information on the specific log management requirements of some of the regulations and industry standards, please see appendix 2, "Compliance requirements for log management."

Since most organizations are subject to multiple regulations and the number continues to grow, organizations need to take a holistic approach to the development of best practices in log management. Contrary to a piece-meal approach, which tries to meet the requirements of each regulation individually, a holistic approach aims to combine efforts and develop best practices which, as much as possible, can address the requirements of multiple regulations and standards and pro-actively plan for future regulations.

### 2. Guidance from legal counsel

Legal counsel should be consulted when developing log management best practices, especially for guidance on developing policies. They can advise not only on the requirements of the applicable regulations, but also any other legal issues or contractual obligations such as business partner agreements which may have provisions for audits (and therefore require access to audit logs). Logs may also be needed as evidence in case of future litigation or investigation. Legal can also help to ensure that log retention policies are consistent with the organization's general data retention policies.

### 3. Business and operational objectives

Best practices in log management should reflect business objectives including working within certain parameters such as available time, resources and budget. Operational objectives could also include improving efficiency of log review; ensuring sufficient monitoring of particular systems to catch problems early and reduce downtime; or keeping certain logs for a particular timeframe in case they are needed for forensics.

### 4. Risk assessment

An essential component of developing a log management competency is a risk assessment. As mentioned previously, neither the regulations nor the standards provide specific requirements. Instead, many decisions must be made by the organization. An assessment of the organization's risks is a key factor in these decisions. The risk assessment can help determine requirements such as how often logs are reviewed and how long certain logs are kept. For example, access logs involving regulated or other sensitive or protected information may require higher levels of scrutiny and longer retention than other logs.

## Recommended Best Practices

A comprehensive set of best practices in log management includes the following categories:

- Logging policy, procedures and technology
- Log generation and capture
- Log retention and storage
- Log analysis
- Log security and protection

[1] Such as European Union Data Protection Directive (EU DPD), Japan Personal Information Protection Act (PIPA), and Canada Personal Information Protection and Electronic Documents Act (PIPEDA)

[2] About 40 states now have laws requiring organizations to notify an individual if there is reason to believe the security of their personal data has been compromised. This set of laws has had a huge impact on organizations worldwide. They do not have direct requirements for log management; however logs are an essential way of detecting a compromise or providing proof that there is no reason to suspect a compromise.

[3] In the EU, the corresponding regulation is the EU's Good Manufacturing Practices (GMP) Annex 11 (Annex 11)

Although best practices should be developed by each individual organization based on their particular environment, there are some general best practices which can be universally applied. RSA has developed a set of 40 recommended best practices covering all of the categories. These best practices are listed below.

## I. Logging Policies, Procedures and Technology (LP)

Policies provide management direction for the log management activities and should clearly define mandatory requirements for log generation, analysis, retention and storage and security. They should be created in conjunction with a plan for the procedures and technology that are needed to implement and maintain the policies.

### Recommended Best Practices

LP1. Provide executive management support for the policies

This should include the necessary prioritization within the organization and the resources required for the log management efforts.

LP2. Fully document the policies and perform periodic reviews and update policies as needed

For example, update the policies and procedures based on results of audits, changes to compliance requirements, and feedback from administrators. At a minimum, policies should be reviewed and updated yearly.

LP3. Define roles and responsibilities and provide proper support for staff

Log management duties should be established across the organization and proper training, tools and documentation should be provided in order to carry out the duties.

LP4. Align log management policies with related policies and procedures

For example, log retention policies should be aligned with general data retention policies. Log management requirements should be factored into procedures such as software procurement and application development.

LP5. Ensure separation of duties

For example, have someone other than a system administrator should review the logs for their system, which ensures accountability for the system administrator's actions.

LP6. Establish standard log management operational procedures to support and maintain the policies

Some typical procedures would include configuring log sources, performing log analysis, initiating responses to identified events, and managing long-term storage.

LP7. Plan and implement a dedicated log management infrastructure to support and maintain the policies

The infrastructure should include a dedicated log management platform and log data storage. By implementing a dedicated log management facility, it is easier for stakeholders to access all the data, perform thorough analysis, ensure robust security, and reliably and consistently store logged data for the appropriate time frames. Without a centrally managed infrastructure stakeholders will likely implement siloed point products that result in inefficiencies, redundancy and increased management complexity.

Organizations need to plan for both the current and future needs including the volume of logs, storage capacity, security requirements, and the time and resources needed for staff to analyze the logs and manage the infrastructure.

LP8. Don't go it alone: leverage an industry expert and/or consultant

Although there are huge benefits to developing a comprehensive set of best practices in log management, it is not a simple task. As this category of best practices demonstrates, it will involve the implementation of policies, procedures and technology. Often organizations do not have the expertise or specialists in-house and would benefit from bringing in an industry expert and/or consultant to help them.

## II. Log Generation and Capture (LG)

Collecting sufficient data to meet the requirements of regulations, potential incident investigations and legal issues is a tall order. For example, privacy regulations expect organizations to maintain a record of all access to personal information. The payment card industry standard requires organizations to track and monitor all access to network resources and cardholder data.

To meet corporate governance regulations, companies must record and store sufficient event data to enable the review, examination and reconstruction of data processing used to generate financial reports. For investigating incidents, organizations need to have a complete historical record of activities within the network, systems and applications. For litigation or human resource issues, organizations need to have the right evidence regarding information use or system access to support their case.

Data must be collected from many sources including security systems, operating and storage systems, and applications. A list of typical sources and contents of logs can be found in appendix 1, "Sources and contents of logs".

### Recommended Best Practices

LG1. Ensure logging is enabled on security systems, network infrastructure devices, storage infrastructure, operating systems and both commercial and custom developed applications

Given the number of systems, devices, and applications, it is important to ensure that audit logging is actually turned on for all of these sources across the organization. Administrators may be resistant to turning on auditing because of fears of a degraded performance but for most systems, if configured properly to work with a robust log management platform, the impact will be minimal. Activation or deactivation of audit control systems should be logged and an alarm message sent to administrators.

LG2. Don't try to filter the logs at the source

Predicting what will be useful or not in today's environment is very difficult to impossible. Wrong decisions can negatively affect audits or investigations. It makes more sense to collect all of the data, and then review it to determine what you don't need versus never collecting it. A well designed log management system can scale to capture, analyze and manage very large volumes of log data, letting you collect all of the data and intelligently purge whatever is assessed as unnecessary later.

LG3. Ensure that data captured includes all of the key event and activity logs required by the standards such as all:

- Individual user accesses
- Rejected system, application, file, or data access attempts and other failed actions
- Privileged, administrative or root access
- Use of identification and authentication mechanisms
- Remote and wireless accesses
- Changes to system or application configurations
- Changes to access rights
- Use of system utilities
- Activation or deactivation of security system
- Accesses to audit logs

LG4. Ensure that details captured for events and activities are in accordance with the requirements of the standards such as:

- Activity or event type (e.g. login attempt, file access, etc.)
- User identification
- Session ID and/or terminal ID
- Network addresses
- Date and time
- Success or failure indication
- Identity or name of affected data, system component, or resource

LG5. Ensure that you are able to track individual users by capturing unique user identification information for all user actions

Especially for systems containing regulated or protected information, you must be able to account for individual user access to information.

LG6. Test your logging facility

It is important to ensure that you are really capturing all the data and that the data in the logs is complete and accurate.

LG7. Synchronize time stamps

Log source typically reference an internal clock when placing a time stamp on a log entry. Ensure all log sources' internal clocks are synchronized to a trusted, accurate time server. A well designed log management system will also time stamp the logs upon receipt and should also be synchronized to a time server.

LG8. Watch for sensitive data collection

Logging can capture (intentionally or inadvertently) sensitive information with privacy or security implications such as passwords or the contents of e-mails. Sensitive information in logs could be seen by those who review the logs or those who gain unauthorized access. A well designed log management system should allow for flexible and comprehensive security in the transport and storage of the log information as well as deliver fine-grained role-based access to insure proper and authorized access to sensitive information.

LG9. Consider privacy issues when setting up user activity logging

Legal counsel should be consulted about appropriate monitoring of employees and other users. Regulations vary considerably by jurisdiction.

## III. Log Retention and Storage (LR)

In determining log retention and storage requirements, consider the stages of logs.

### Data stages

1. Production data – is data being actively used for real-time analysis, on-going review and periodic audits and assessments
2. Backup data – is a mirror image of the production data that may be needed in case the production data is compromised or damaged
3. Active archive data – is a sub-set of the production data which will be stored longer-term for record-keeping purposes based on regulatory, legal discovery and possible forensic requirements

Also consider how the data will be stored. There are different types of storage which provide for different levels of accessibility, for example:

### Storage mechanisms

1. On-line storage – data is stored on high-performance networked storage systems with access times measured in a few milliseconds providing constant availability to a large number of users
2. Near-line storage – data is stored on a storage subsystem with access times measured in a few seconds providing infrequent availability for a small number of dedicated users for very long periods of time
3. Off-line storage – data is stored to disks and tapes that are kept in a data library and cannot be accessed from a computer until mounted

To make decisions regarding retention time frames and storage mechanisms, organizations need to look at:

1. Why are the logs needed?
2. When do logs need to be accessed?
3. How far back do they need to go?
4. How accessible do they need to be?

The three tables below examine these issues for each of the three stages: production, back-up and active archive data.

### Table 1: Production Data

| Why are logs needed? | When do logs need to be accessed? | How far back do they need to go? | How accessible do they need to be? |
|---|---|---|---|
| Log reviews and analysis | Very frequently (e.g. real-time, daily, weekly, monthly, etc.) | Since the last review | Need fast access to facilitate quick analysis |
| Forensic investigations | – Security incidents and data leaks, etc. may occur at any time so investigations may need to occur at anytime<br>– Logs will likely require periodic access (possibly frequent) | – Attacks can be perpetrated over a long period (e.g., a recent high-profile attack occurred over a period of 18 months)<br>– May need to go back into certain logs as far back as one year or longer | Need fast access to determine causes of breaches quickly |
| Internal audits | – Frequency of access depends on length of audit cycle<br>– May vary by industry<br>– Typical internal audit cycles for large enterprises can be 3 months (e.g. financial services) to 6 months (e.g. retail)<br>– Some high risk areas may be audited more frequently than audit cycles | – Need to go back as far one audit cycle and a minimum of one quarter to ensure that the complete record of logs for the audit cycle is available<br>– Typically 6–9 months | Need fast access to ensure productivity of internal auditors |
| External audits/ independent assessments | – Depends on length of audit cycle<br>– For many regulations external audit cycles are one year for example:<br>SOX requires annual assessment<br>GLBA requires board review of security controls once per year<br>FISMA requires an annual review<br>PCI requires annual self-assessment or on-site audit<br>NERC has a specified compliance review timeframe of 1 year<br>EU Data Protection Directive Safe Harbor requires yearly audits<br>For some global privacy regulations, audit cycles may be longer, for example, ISO 17799/27001 requires re-certification every 3 years<br>For Part 11/Annex 11, depends on predicate rules regarding inspections<br>FTC rulings have required independent audits once every 2 years | – Need to go back as far one audit cycle and a minimum of one quarter to ensure that the complete record of logs for the audit cycle is available<br>– For most regulations, this means one year + 3 months = 15 months<br>– Most regulations do not specifically indicate retention durations of logs for audit cycles, except:<br>– PCI specifies that an audit trail must be retained for at least 1 year with a minimum of 3 months on-line<br>– NERC requires organizations can prove there have been no gaps in monitoring or logging over a full year (which contradicts the other record-keeping requirement which states logs be kept for a minimum of 90 days) | Need fast access to ensure productivity of auditors or assessors and minimize audit costs |

Table 2: Back-up Data

| Why are logs needed? | When do logs need to be accessed? | How far back do they need to go? | How accessible do they need to be? |
|---|---|---|---|
| In case production data is compromised or damaged, etc. | – Data compromises or damage may occur at anytime<br>– Likely will not require frequent access | Should mirror the production data | Access does not need to be immediate, but logs should be reasonably accessible. |

Table 3: Active Archive Data

| Why are logs needed? | When do logs need to be accessed? | How far back do they need to go? | How accessible do they need to be? |
|---|---|---|---|
| Record-keeping to meet regulatory, legal discovery and possible forensic requirements | – May need to produce records at any time in response to regulatory requests, legal discovery, or investigations<br>– Likely will not require frequent access | – As noted above, PCI requires logs be retained for a minimum of 1 year; considering the frequency of cardholder data breaches, organizations should consider longer-term retention periods in order to have the data available for forensics<br>– For most regulations, no definitive timeframe for long-term log retention is provided but a more general record retention timeframe often is which can be used in guiding long-term retention requirement for logs<br>– SOX requires documents and communications related to an audit are kept for 7 years; organizations typically select certain logs to retain longer term such as those directly related to proving the integrity of financial reports (e.g. access logs to key financial applications)<br>– HIPAA requires retention of documentation of policies, procedures, actions, activities or assessments for 6 years; organizations typically select certain logs to retain longer term such as those directly related to accessing patient information (e.g. access logs to medical records)<br>– For FISMA, NIST is the applicable standard, which requires certain logs be kept for 3 years<br>– NERC requires audit records be kept for 3 years<br>– Under global privacy regulations, in cases of privacy breaches, organizations may need to produce evidence of access to personal information going back several years<br>– For other regulatory requests and legal discovery, log retention should align with the corresponding data or record retention policies which could be several years<br>– Organizations should also look at retaining certain logs longer-term so that they are available for potential investigations in case of a security breach | Access does not need to be as quick as for production data and also will depend on age of records; more recent logs should be more accessible than older logs |

*Log Retention and Storage (LR), continued*

## Recommended Best Practices

### LR1. Retain logs in a secure, well managed storage infrastructure

A streamlined, centrally managed storage system is less complex to manage than a piecemeal collection of storage subsystems and eliminates the inefficiencies associated with silos of logged data. Centralized management and storage of logs also facilitates access to logged data collected from across the organization. Rather than each stakeholder deploying their own logging system, a well designed log management system should provide stakeholders with secure, fine-grained, role-based access to all of the stored logs. This way, stakeholders get access to all of the data they need and the organization optimizes log storage.

### LR2. Use an information lifecycle management approach whereby logged data is stored relative to access requirements

Data that requires frequent or ready access such as production data should be available on-line while data not requiring as frequent or ready access such as back-up and active archive data can be stored near-line or off-line.

### LR3. Retain production data on-line for one year and one quarter = 15 months (minimum)

Providing on-line access to production data enables frequent use for real-time monitoring and on-going review and analysis. In case of a security breach, the logs are readily accessible so that investigators can quickly determine the reasons for the compromise or source of the data leak, and remediate their systems or solve the security issues (faster investigations also make finding the culprits easier). Retaining logs for at least this timeframe is important for ensuring the right evidence will be available.

A 15-month on-line retention period also ensures that the complete record of logs is available and readily accessible for the internal audits as well as external audits or independent assessments. As indicated in the above table, most regulations have a one-year audit cycle associated with them. It is prudent for organizations to have a one year + a minimum of one quarter retention period to meet the one-year audit cycles. The extra quarter provides a necessary "buffer" as audit cycles vary from year-to-year and from regulation-to-regulation.

Since most organizations are subject to multiple regulations, most will need to have logged data on hand for multiple audits or assessments per year. By having the data on-line, organizations can pro-actively manage the audit process, increase the productivity of auditors, and minimize the time and costs of audits.

### LR4. Retain back-up data near-line for the same period as production data

This ensures that the back-up data would be available in case the production data is compromised or damaged, etc. but it does not need to be as accessible as production data.

### LR5. Retain active archive data for approximately 2 – 7+ years (minimum) using near-line storage for more recent records (e.g. up to 5 years) then possibly moving some records to off-line storage (e.g. 5 years +)

As indicated in table 3 on the previous page, most regulations do not provide definitive time frames for retaining audit logs. Organizations will typically keep certain logs after an audit cycle for several years, especially those directly related to accessing applications containing protected data. Organizations will not only have regulatory requirements but also other requirements for keeping log data long term such as legal discovery and forensic investigations.

Because it will not be used frequently, archive data does not have to be accessible on-line. However, organizations should make records fairly accessible, so that responding to regulatory requests, producing records for legal discovery or conducting investigations does not take an inordinate amount of time. Content-addressable storage should also be considered for longer-term storage to ensure the integrity of the information is protected over long periods of time.

### LR6. Ensure log retention policies are developed in consultation with legal counsel

It is essential that legal counsel be consulted in developing log retention requirements, which must be aligned with the organization's general data retention policies.

### LR7. Address the preservation of original logs

In cases where logs may be needed as electronic evidence for regulatory purposes, legal proceedings or even to support internal HR-related actions, a well-designed log management system should facilitate the management and archival of the original log files.

### LR8. Ensure retired logs are disposed of

Ensure that when the required data retention period has ended, the logs are retired by destroying them according to the organization's data destruction policies.

## IV. Log Analysis (LA)

Given the volume of data, monitoring and reviewing logs is a daunting task. Some companies collect logs but they do not review them simply because it is too hard. Others have administrators spending inordinate amounts of time reviewing large volumes of logs. Yet without good analysis, the value of the logs is significantly reduced.

The current regulatory environment and threat landscape demands that organizations carefully monitor logs to detect unauthorized intrusions and enforce user accountability. Log analysis best practices must address the need to make analysis easier, enabling the organization to extract the wealth of information logs can provide.

### Recommended Best Practices

LA1. Regularly review and analyze logs

Regular review and analysis will help to identify for example, anomalous events on the network or user behavior that is outside of policy. Depending on the systems, risk environment, and other requirements, logs should be reviewed in real-time, daily, monthly, or every 90 days. Some regulations and standards have specific requirements regarding the review of logs (for more information see appendix 2, "Compliance requirements for log management").

LA2. Aggregate logs using centrally managed log management infrastructure

When logs are aggregated, analysis becomes easier and will be done more reliably.

LA3. Automate as much of the log analysis process as possible

Automation can significantly improve analysis, since it will take much less time to perform and produce more valuable results. Manually analyzing log data is often perceived by administrators as uninteresting and inefficient and is often treated as a low-priority task and therefore not done or not done well or consistently. This should include using automated, interactive systems to track what logs have been reviewed. A more automated review process can free personnel from manual review, allowing them to do higher value tasks.

LA4. Leverage correlation tools to attain a holistic view and reduce false positives

Most organizations have many different systems generating logs including security systems; operating and storage systems; and applications. Reviewing logs from many systems separately is difficult, inefficient, and can create voids. Attacks often involve multiple assets; if you watch only one in isolation, a single activity may not seem threatening. Correlation tools look for patterns of events across multiple systems. They are particularly helpful in helping to reduce false positives.

LA5. Use automated reporting tools to facilitate review of logs though report generation

A reporting process should define content of reports as well as how often they are generated and for what purposes.

LA6. Review procedures should include real-time monitoring of applicable log events

Traditionally, most logs have not been analyzed in real-time, however it is key to detecting attempts at unauthorized intrusions and activities and preventing these or at least minimizing them.

LA7. Set up an alerting system based on priorities

Personnel should know what to do when suspicious anomalous activity is identified. Keep in mind that you will not want to alert on everything or it defeats the purpose and personnel will end up not paying attention. Prioritize what really requires alerts.

LA8. Develop a baseline of typical log entries in order to detect unusual or anomalous events or activities

By determining which types of log entries are of interest and which are not, malicious events can be recognized more easily and responded to more quickly.

## V. Log Security and Protection (LS)

Best practices must ensure the confidentiality, integrity and availability of logs throughout their lifecycle. The organization must prevent the logging mechanisms from deactivation or compromise, ensure that log files cannot be edited or deleted, and provide for business continuity of logging services in the event of an incident.

Logs that are secured improperly in storage or in transit might be susceptible to intentional and unintentional alteration and destruction. This could allow malicious activities to go unnoticed and evidence to be manipulated concealing the identity of a malicious party. (For example, many root kits are specifically designed to alter logs to remove any evidence of the root kits' installation or execution.)

### Recommended Best Practices

**LS1. Secure the processes that generate the log entries**

Unauthorized users should not be able to manipulate log source processes, executable files, configuration files, or other components of the log sources that could impact logging. All management of log generation sources should also be logged and controlled via approved change control policies and procedures.

**LS2. Limit access to log files**

Generally only administrators and auditors should have access to log files for review and management only. All privileged user (i.e. the administrator and auditor) access should be logged and reviewed thoroughly and frequently by others outside that user domain.

**LS3. Implement secure mechanisms for transferring log data**

Many logs are sent in clear text. Communications should be protected with mechanisms such as encryption (e.g. IPSec. SFTP or SSL).

**LS4. Protect log files in storage**

This includes limiting access to storage mechanisms to authorized users, providing adequate storage capacity and leveraging Write Once Read Many technologies.

**LS5. Protect the confidentiality and integrity of log files**

Message digests, encryption, and/or digital signatures can be used.

**LS6. Provide adequate physical protection for logging mechanisms and stored logs**

This includes preventing unauthorized physical access and ensuring proper environmental controls.

**LS7. Maintain business continuity for logging services**

Counteract interruptions to business activities by ensuring that in the event of a disaster or computer failure the logging services can be restored in a timely manner through redundant log servers.

## Conclusion

Developing best practices in log management is not a simple task. It will require a commitment of resources and considerable effort. By providing a set of recommended best practices covering all of the major components of log management, this paper should help ease the effort involved in developing a log management capability. This is becoming critical as the regulatory environment and the threat landscape are demanding more intensive logging and longer-term retention and storage of logs than most organizations are able to do. But meeting compliance and security requirements must be aligned with business objectives. Fortunately, a robust log management capability will also enable increased efficiency, productivity, and cost savings in areas across the organization; providing a healthy return-on-investment.

## Solutions for Implementing Best Practices

Implementing best practices in log management establishes the foundation for comprehensive security information and event management (SIEM). RSA provides end-to-end solutions which enable organizations to build a centrally-managed dedicated infrastructure. RSA enVision SIEM platform aggregates logs from across the enterprise, and turns this information into actionable intelligence for compliance and security. By combining RSA enVision with networked storage solutions, organizations can manage the entire information lifecycle of logs using a tiered storage approach, whereby logs are stored on different storage resources based on the age of and need for the log data.

The RSA enVision platform works seamlessly with EMC Celerra®, Clariion®, Symmetrix® and Centera® storage for an end-to-end solution in information lifecycle management for log data. This solution enables organizations to manage the huge volumes of log data from creation to deletion in order to meet regulatory compliance, security operations, and business requirements.

For more information on RSA enVision, please go to www.rsa.com. For more information on EMC's storage solutions including EMC Celerra, Clariion, Symmetrix and Centera, please go to www.emc.com.

## Appendix 1: Sources and Contents of Logs

| Security Systems and Software | Examples of event or activity recorded |
|---|---|
| **Anti-malware software** — such as anti-virus, anti-spyware and root kit detectors | – Instances of detected malware<br>– File and system disinfection attempts<br>– File quarantines<br>– Malware scans<br>– Signature or software updates |
| **Intrusion detection and intrusion prevention systems** | – Suspicious behavior<br>– Detected attacks<br>– Actions performed to stop malicious activity |
| **Remote access and wireless access systems** — such as virtual private networks (VPN) | – Login attempts<br>– Amount of data sent and received during session |
| **Web proxies** | – URLs accessed |
| **Vulnerability Management Software** — includes patch management and vulnerability assessment software | – Patch installation history<br>– Vulnerability status<br>– Known vulnerabilities<br>– Missing software updates |
| **Authentication Servers** — includes directory servers and single sign-on servers | – Authentication attempts |
| **Routers and switches** | – Blocked activity |
| **Firewalls** | – Detailed logs of network activity |
| **Network quarantine servers** | – Status of host security checks<br>– Quarantined hosts and reason |
| **Operating Systems** | **Examples of event or activity recorded** |
| — such as those for servers, workstations and networking devices (e.g., routers, switches). | – System Events<br>System shut down<br>Service starting<br>– Security events<br>File accesses<br>Policy changes<br>Account changes |
| **Applications** | **Examples of event or activity recorded** |
| — such as e-mail servers and clients, Web servers and browsers, file servers and file sharing clients, database servers and clients and business applications (e.g. supply chain management, financial management, procurement systems, enterprise resource planning, customer relationship management and custom-developed applications) | – Client requests and server response<br>– Authentication attempts<br>– Account changes<br>– Use of privileges<br>– Number and size of transactions<br>– Operational events<br>Startup and shutdown<br>– Configuration changes<br>– Application-specific events such as:<br>Email sends and receipts<br>File access<br>Service request<br>Transaction<br>Function performed (such as read, write, modify, delete) |

## Appendix 2: Compliance Requirements for Log Management

Note: Not exhaustive, simplified for presentation)

| | Examples of legislation or regulations mandating information protection | | | | | Industry and information security standards | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | Sarbanes-Oxley (SOX) | Industry-specific privacy[1] | Federal Information Security Management Act (FISMA) | Global Privacy[2] | 21 CFR Part 11 (FDA)/ Annex 11 (EU) | Payment Card Industry (PCI) Data Security Standard (DSS) | International Standards Organization "Code of Practice for Information Security Management" ISO 17799/27001 | North American Electric Reliability Council (NERC) Cyber Security Standards | National Institute of Science and Technology Special Publications 800 Series (e.g. 800-53, 61, 66 & 92) | Federal Financial Institutions Examination Council IT Handbook on Information Security (FFIEC) | Control Objectives for Information Technology (COBIT) |
| Relevant standard (if applicable) | COBIT | NIST SP 800-66 for HIPAA, FFIEC for GLBA | NIST SP 800 (esp. SP 800-53) | ISO 17799/27001 | ISO 17799/ 27001 | | | | | | |
| Protected information | Financial systems and information used to generate financial reports | E.g., protected health information, consumer's personal financial information | Federal information | Personal information | Electronic records used in developing and mfg drugs | Cardholder information | ORG | Critical cyber assets[3] that control or could impact the reliability of the bulk electric systems | ORG | ORG | ORG |
| **Requirement – what to log (examples)** | | | | | | | | | | | |
| Individual user access to protected information | N/S | Indicated[4] | Indicated[5] | Indicated[6] | R[7] | R | R | R | R | R | Indicated[8] |
| Administrative actions and use of privileged access | N/S | N/S | N/S | N/S | N/S | R | R | R | N/S | R | N/S |
| Invalid access attempts | N/S | Indicated[9] | N/S | N/S | N/S | R | R | R | N/S | R | N/S |
| Security system events[10] | N/S | N/S | N/S | N/S | N/S | R | R | R | R | R | Indicated[11] |
| Access to audit trails | N/S | N/S | N/S | N/S | N/S | R | R | N/S | R | R | N/S |
| Review logs at specified time intervals | N/S | HIPAA requires regular review of audit logs | N/S | N/S | N/S | Daily reviews of logs and 24/7 monitoring for unauthorized access | Periodic and regular reviews; more for privileged user access | Review of logs at least every 90 days and 24/7 monitoring for unauthorized access | Regular review of audit logs required; for HIPAA, 800-66 requires log review twice per week | Regular and timely review required which could be daily reviews of some logs and real-time monitoring of others | N/S |
| Log aggregation, correlation and automation of audit logs | N/S | N/S | N/S | N/S | N/S | REC | REC | REC | REC | REC | REC |
| Security and protection for logged data | N/S | N/S | N/S | N/S | N/S | R | R | N/S | R | R | N/S |
| Time stamps and/or synchronization | N/S | N/S | N/S | N/S | R | R | R | R | R | R | N/S |

*– continued*

Legend

N/S = not specified
R = required
ORG = organization-defined
REC = recommended

## Retention

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Minimum specified duration | N/S | N/S | N/S | N/S | N/S | At least 1 year | ORG | Minimum of 90 days | ORG | ORG | ORG |
| Retention needed to meet audit cycle (independent assessment) | 1 year: Annual assessment of internal controls | 1 year: Require mandatory periodic review of security: common cycle is one year[12] | 1 year: Evaluation of security controls is required annually | 1 to 3 years: Audits or assessments required every one–three years[13] | Varies: Subject to periodic inspection by regulating agency | 1 year: Annual self-assessment or on-site audit | N/S | 1 year: Compliance review time-frame is 1 year; must be able to prove no gap in logs over 1 year period | N/S | Based on risk analysis: quarterly internal audits and yearly independent audits recommended | Sufficient retention required[14] |
| Long-term retention of records that may include audit logs | 7 years[15] | 6 years for HIPAA; N/S for GLBA[16] | N/S | N/S | Depends on predicate rule for retaining subject electronic record; could be many years[17] | Not specified; although retention requirement is *at least* 1 year | N/S | Audit records must be kept for 3 years | Certain logs should be retained for 3 years | N/S | N/S |

## Notes to Appendix 2 Table

[1] Such as Health Insurance Portability and Accountability Act (HIPAA) and Gramm-Leach-Bliley Act (GLBA)

[2] Such as European Union Data Protection Directive (EU DPD), Japan Personal Information Protection Act (PIPA), and Canada Personal Information Protection and Electronic Act (PIPEDA)

[3] Computers, software and communication networks

[4] The kind of audit logs to collect is not specified but logging individual access to data is indicated by both HIPAA and GLBA based on the requirements for access controls, identifying individual users and audit controls to monitor and examine system activity such as access reports

[5] FISMA does not specify the kind of audit logs to collect, but logging individual access to data is indicated since it has general requirement for protection from unauthorized access using appropriate levels of information security; it is difficult to impossible to protect data from unauthorized access unless a record of who accessed the information is kept

[6] Although global privacy regulations do not specify the kind of audit logs to collect, logging individual access to data is indicated by all of them since they have a general requirement for protection from unauthorized access using reasonable and appropriate measures; it is difficult to impossible to protect data from unauthorized access unless a record of who accessed the information is kept

[7] Part 11 requires limiting system access to authorized individuals and use of secure, computer-generated, time-stamped audit trails to independently record the date and time of operator entries and actions that create, modify, or delete electronic records.

[8] COBIT does not require logging of individual user access to data but it requires controls to uniquely authenticate users and to log security activity at the system, application and database levels

[9] "Procedures for monitoring login attempts and reporting discrepancies" is an addressable implementation specification under HIPAA

[10] Could include various logs from security systems such as anti-malware, firewalls, intrusion detection/prevention systems, virtual private networks, vulnerability management software, and authentication servers

[11] COBIT requires appropriate controls, including firewalls, intrusion detection and vulnerability assessments exist and are used to prevent unauthorized access via public networks.

[12] Most organizations do an annual review of security controls (board is required to review security every year for GLBA)

[13] EU DPD Safe Harbor process requires yearly audits; applicable standard is ISO 17799/27001 which requires re-certifications every 3 years after initial certification

[14] COBIT requires that system event data are sufficiently retained to provide chronological information and logs to enable the review, examination and reconstruction of data processing.

[15] SOX requires documents and communications related to an audit are kept for 7 years but does not specify log retention; organizations typically select certain logs to retain longer term such as those directly related to proving the integrity of financial reports for example access logs to key financial applications

[16] HIPAA requires retention of documentation of policies, procedures, actions, activities or assessments for 6 years but does not specify log retention; organizations typically select certain logs to retain longer term such as those directly related to accessing and/or disclosing patient information such as access logs to medical records

[17] Part 11 requires audit trail documentation be retained for a period at least as long as that required for the subject electronic records and shall be available for agency review and copying.