

# Control Essentials

Volume II, Issue VI

June 2007

## Business Consulting

- Regulatory Support
  - Policies and Procedures
  - Regulatory Compliance
    - Sarbanes-Oxley
    - GLBA
    - HIPAA
    - BSA
  - PCI (Payment Card Industry) Security Audit
  - Information System Audit Outsourcing
- Enterprise Support
  - Business Continuity Planning
  - Attestation and Assurance
    - SAS-70
  - E - Discovery
  - Forensic Examinations
  - Security Remediation

## Technology Consulting

- Application Security
  - Application Security Assessment
  - Application Penetration Test
  - Web Application Security Assessment
  - Web Application Penetration Test
- Network Security
  - Risk Assessment
  - Vulnerability Assessment
  - Penetration Testing
    - Internal
    - External
    - Social Engineering
    - War Dialing
    - War Driving
    - Blue Snarfing
  - Wireless Security Assessment
  - Information System Security Audit
  - Information System Control Audit
  - Network Architecture Design and Assessment
  - Physical Security Assessment
  - Log Analysis

## Watch Your Logs!

Security logs are files containing information about events that occur within the network, systems and applications of an organization. They are comprised of a number of log entries, each referring to details pertaining to a specific event. Security logs provide administrators with a precious means to monitor the security of the system and identify operational problems. They are used to record user actions, perform auditing and forensic analyses, and detect security incidents such as policy violations. In addition, the review of security logs is strongly recommended by Federal regulations such as the FISMA, GLBA, BSA, SOX, HIPAA and the Payment Card Industry Data Security Standard.

### Security Logs: Policies and Procedures

Organizations must create and document formal policies, standards and procedures for log management activities. This practice promotes a consistent approach towards log management throughout the organization and ensures compliance with laws and regulations. Essential topics that need to be addressed in these documents include review process, retention period, location of online and offline logs, and the staff in charge of reviewing the log records.

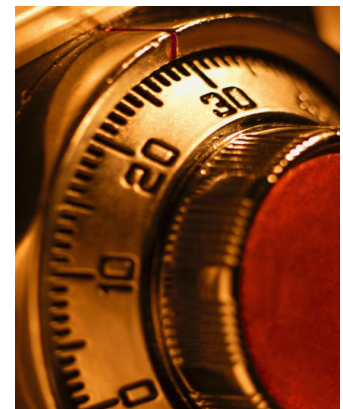
### Security Logs: Configuration

The security logs of all network components, operating systems, subsystems such as databases, program change systems and applications should be active and monitored. Administrators need to determine the information to be logged and estimate how much space the log will require. Sufficient resources should be allocated in order to ensure that the logging information is not overwritten. Typically, the space allocated should allow for the capture of online logging information for a period of five days after which a backup is created for offline storage.

Data retention best practices recommend that organizations maintain copies of log files for a minimum of 3 months. Also, current industry best practices recommend that the logs be retained for a period of 6 months in order to support computer or network crime investigations that the organization may have to face. In order to comply with these requirements and to ensure confidentiality and integrity of the log information, off-line logs should be stored in a secure location with a strong physical access control mechanism.

### What information needs to be recorded in a log?

The format of a security log may vary depending on the source of the log. Logs generated by security software such as antivirus software, firewalls, intrusion detection systems, or authentication servers may differ from those created by operating systems or applications. Log formats may also be vendor specific. This lack of standardization combined with the large number of log information sources produces inconsistencies and incompatibilities in content and format that make it difficult for administrators to analyze the collected data. This is the reason why some organizations utilize automated methods to consolidate multiple logs into a single standard that can be easily analyzed.



Regardless of the format and source, all logs should record at least the following activities:

- User logins and logouts
- Configuration changes
- Administrative account logins and logouts
- Failed access to critical folders, files and other critical resources
- Changes to users, groups, services and other critical resources
- All suspicious activities such as:
  - Switching userID during an online session
  - Guessing passwords
  - Attempting to use unauthorized privileges



## Review of Security Logs

Security personnel and network administrators usually manage network and security devices and thus they need to analyze the log information and report issues to management. Typically, administrators review logs once a week. However, it is highly recommended to review logs on a daily basis. Organizations also need to monitor administrators' actions to ensure accountability and reduce the probability of internal criminal activities. This can be achieved by enforcing dual control i.e., by having more than one person review the logs.

There are two main approaches to review a security log: real time and batch mode. In real time reviews, the software applications that analyze the logs notify the administrators about any unusual event as soon as it occurs. This is in contrast to the batch mode, where a report is generated periodically so that it can be analyzed at the administrators' convenience.

While reviewing security logs, the most challenging activity is "event correlation" which refers to the identification of common factors between two or more log entries. Event correlation usually requires statistical tools to discover patterns that would normally be overlooked by the human eye. However, human knowledge and experience are essential to interpret the results of the tools and distinguish the false positives from the significant findings. Events correlation requires administrators to ensure that the event time stamps collected from the systems involved in the analysis are synchronized and that sufficient logging activities are available.

## Regulatory Compliance

Organizations that need to comply with federal legislation and regulations must review log information on a regular basis. The requirements for each regulation are discussed below:

### Federal Information Security Management Act (FISMA)

The motivation behind FISMA was to secure computer systems and networks within the Federal Government and its affiliates. The FISMA Act requires federal agencies to develop, document, and implement an organization-wide program to provide information security for their information systems. Security log retention and review are a significant part of the overall security requirements. *NIST SP 800-53, Recommended Security Controls for Federal Information Systems* defines several controls for proper log management that are part of the compliance requirements of FISMA.

### Gramm-Leach-Bliley Act (GLBA)

The GLBA requires financial institutions to protect Non Public Customer Information from unauthorized access and use. Security logs can be used by organizations to detect security incidents affecting customer information. In the case of an incident, a financial institution can determine which customer's information has been accessed in an unauthorized manner by reviewing its logs. The institution now has the option of notifying only those customers that are affected, or could be affected under the judgment of reasonable possibility. In the absence of such a mechanism to single out affected customers, the institution is required to inform all the customers.

### **Bank Secrecy Act (BSA)**

Banks are subject to stringent anti-money laundering laws such as the Bank Secrecy Act of 1970 which establishes that banks must maintain records and report all suspicious activities to law enforcement agencies. Banks that do not meet stipulated requirements may be subject to fines of up to \$1 million a day.

Logs are a reliable source to identify money laundering activities since they can be used to trace the source and the routes of money transferred over the Internet. Hackers can take over an innocent server to send out cash transfer orders and masquerade as another person. However, logs would fingerprint the activities of the hacker on the server as well as the actual origin of such activities. The trail of transactions across all the servers on the Internet can then be used by forensic investigators to track down the hacker.

### **Sarbanes-Oxley Act (SOX)**

Organizations requiring compliance with the SOX Act would need to review their logs on a regular basis to detect potential security breaches and retain records of log reviews for future assessments by auditors. Organizations would do good to record relevant system events such as shutdowns, restarts and any other unusual events. Additionally, the SOX Act requires log information be kept confidential and disclosed only to authorized personnel.

### **Health Insurance Portability and Accountability Act (HIPAA)**

HIPAA requires healthcare organizations to protect personally identifiable health information. These organizations would be greatly benefited by regular reviews of audit logs and access reports. Software systems dealing with medical information need to generate detailed audit information that describes how a user accesses and utilizes resources. HIPAA also requires that logs are backed up on a regular basis and retained for at least 6 years.

### **Payment Card Industry Data Security Standard (PCI DSS)**

The PCI DSS requires all organizations that process and transmit credit card information to monitor access to the network resources and card holder information. Logging and audit trails must be enabled and needs to be unique to each entity's cardholder data environment. This provides for timely forensic investigation in the event of a computer crime or fraud. Compliance with the PCI standard applies to merchants and service providers regardless of the method of payment (Telephone, e-commerce, mail, etc.).

### **Conclusion**

Logs serve as one of the primary sources of information for system administration support. The importance of log retention and review are highlighted by the log management requirements imposed by the numerous laws, regulations and standards governing organizations in different industries. These requirements serve to provide organizations with the impetus to monitor logs. Compliance aside, it is the responsibility of every organization to monitor network, system and application activities to ensure the highest level of security of confidential information and this should be reason enough to implement log management.

Enterprise Risk Management, Inc. (ERM) professionals have expertise in information security. ERM assists many types of organizations in complying with laws related to information security. ERM does not provide legal advice.

## **LogWatch - Enterprise Risk Management's Unique Log Review Service**

Enterprise Risk Management can help you with your periodic log review needs with a service tailored to meet your needs -

- ✓ Upload your logs to the Secure ERM Server
- ✓ Download Reports within 24 Hours
- ✓ Affordable and Efficient
- ✓ One of ERM's most popular services

# Enterprise Risk Management At A Glance

ERM professionals bring a unique mix of strong academic backgrounds complemented by professional experience ranging from "Big Four" consulting firms to major corporations and prestigious professional certifications. A snapshot of ERM's profile can be seen below:

## Education

### Qualifications

M. S. in Computer Information Systems  
M. S. in Information Networking  
M. S. in Management Information Systems  
Master of Accounting Information Systems  
Master of Business Administration

### Universities

Carnegie Mellon University, Pittsburgh, Pennsylvania  
Syracuse University, Syracuse, New York  
Xavier University, Cincinnati, Ohio  
University of Miami, Miami, Florida  
Florida International University, Miami, Florida

## Certifications

Certified Public Accountant (CPA)  
Certified Information Systems Security Professional (CISSP)  
Certified Information Systems Auditor (CISA)  
Certified Information Systems Manager (CISM)  
Certified Information Technology Professional (CITP)  
GIAC Security Essentials Certification  
GIAC Systems and Network Auditor  
Microsoft Certified Professional

## Prior Work Experience

PriceWaterhouse Coopers  
CERT® Coordination Center  
SONY Electronics Latin America, Inc.  
RJR Nabisco  
Diageo plc  
Arthur Young  
Carnegie Mellon CyLab  
Evertec Inc.  
American Bankers Insurance Group  
Chesebrough Pond's  
Starboard Cruise Services, Inc.  
Demotte Consulting, Ltd.

## Some of our Clients...

ABN AMRO Private Banking  
Bacardi-Martini, Inc.  
CitiBank  
Carnival Cruise Lines  
Commerce Bank  
Florida Power & Light Company  
Knight Ridder  
North Broward Hospital District  
Ocean Bank  
Rinker Materials  
Sylvania Lighting International  
The International Bank of Miami

We encourage you to visit our website, [www.emrisk.com](http://www.emrisk.com), for details on ERM's services, team profile, clientele and testimonials from some of our clients.

For further information, please contact an ERM consultant at (305) 447-6750.