

# On the Trail of Trust : Transactional Integrity, Secure Audit Logging and Compliance

A Whitepaper by Kinamik



© Kinamik Data Integrity, 2007

## Contents

Introduction .....	2
The Case for Increasing Accountability-Reducing Compliance Costs.....	3
Characteristics of Secure Audit Logging -How Do I Know I Can Trust My Audit Log? .....	5
Business Applications/Databases - Secure Audit Integration .....	7
Compliance- Secure Logging / Transaction Integrity .....	9
Conclusion .....	12

Note: A detailed analysis on Compliance, Forensics and Governance can be found in a separate Appendix to this document.

## Introduction

Companies that are under competitive pressure and/or stringent compliance and legal guidelines are using strong accountability mechanisms, specifically, secure audit trail/logging<sup>1</sup> to provide the ability to reliably reconstruct and *irrefutably* prove the integrity, origin, order and sequence of events contained in audit logs in support of business operations. This same technology has application; in general, to preserving electronic records integrity, for example in ensuring reliable transport of multimedia streaming digital content. This concept can be extended to other applications including the need that e-government be accountable to citizens by providing an independent record of e-government/citizen electronic transactions. Also, there is a growing need by businesses that rely on e-commerce for highly reliable tracking of electronic transactions and intra/inter company information sharing of electronic documents. Not to mention protecting private information such as user names, passwords, credit cards data that may inadvertently get recorded in system logs. Without this ability, even a significant time after an incident has taken place you have a significantly weaker case when it matters most in proving compliance, the trustworthiness of legal evidence, and performing meaningful forensics. Secure audit logging can be used by companies of any size to increase their competitiveness, raise corporate confidence in the use of new business models such as Web 2.0 information sharing and collaborative technology while ensuring individual accountability, transaction integrity and reduced compliance costs. This document will talk about the role of secure logging as an integral part of a business risk management strategy in the following areas – compliance, governance and application integration.

---

<sup>1</sup> NIST, <http://csrc.nist.gov/publications/nistpubs/800-12/800-12-html/chapter18.html>, section “18.3.1 Protecting Audit Data”, Last Accessed: 12 Aug 07

## The Case for Increasing Accountability-Reducing Compliance Costs

Maintaining a high level of assurance of the trustworthiness of critical logs and transactional integrity, being able to maintain a reliable record of electronic interactions for the duration of the information lifecycle, means companies can have the confidence to offer more value and service to customers and business partners while reducing administrative burden and compliance costs. Having this kind of competitive advantage is especially important in the face of the threat of undetected data leakage, unauthorized activities of trusted insiders<sup>2</sup> and increasing compliance obligations and need for trustworthy forensics.

Clearly, data protection plays a key role in encouraging the increased information sharing between businesses and their customers and partners. However, treating employees, customers, and partners who have access to this information as traitors-in-waiting is unlikely to be effective. Therefore collaborative value must be created by providing these constituents with information access while maintaining strict accountability.

Accountability means holding people responsible for the things they do. In the world of information technology this often involves logging user activity. Accurate, tamper proof audit trails play a key role in user accountability, system reliability, and forensics.

Secure audit logging, meaning that such logs of electronic transactions meet a high legal standard of trustworthiness and credibility provides a reliable accountability

---

<sup>2</sup> Organized Crime Infiltrates Financial IT, InfoWorld.com, Matt Hines, July 23, 2007  
[http://www.infoworld.com/article/07/07/23/Organized-crime-infiltrates-financial-IT\\_1.html](http://www.infoworld.com/article/07/07/23/Organized-crime-infiltrates-financial-IT_1.html) Last

mechanism for proactively monitoring and forensically establishing access and use of critical, high risk information. This is especially important consideration for companies in industries that deal with a high volume of sensitive information and are operating under stringent regulatory environments. The variety of companies that have been recent cyber crime victims means that the size of a company is no longer a reliable predictor of which company, large or small, will fall victim and need the ability to raise the level of internal and external trust of its audit log data for compliance and forensics<sup>3</sup>. If sufficiently strong accountability mechanisms over critical, high risk information systems are not proactively built in to a company's risk reduction strategy business risk could increase in a number of areas including, incident recovery costs, lost revenue, losing customer trust, proving compliance, defending human resource actions, forensics and the ability to wage successful litigation.

Auditor costs can be minimized by demonstrating to auditors that IT systems security goes beyond minimal compliance and seek to follow the 'spirit' of the regulation in keeping with your business objectives. For example in the area of logging and incident response/forensics implementing secure logging of critical user and system electronic transactions demonstrates an element of a truly risk-based security program; resulting in increased auditor comfort level; auditor doesn't have to look so hard; reduces audit time/costs. Costs can further be reduced by leveraging security controls such as secure logging across multiple systems to meet multiple regulatory compliance objectives.

---

<sup>3</sup> FBI goes on offensive against China's tech spies, <http://www.usatoday.com>, David Lynch, July 24, 2007, [http://www.usatoday.com/money/world/2007-07-23-china-spy-2\\_N.htm?csp=34](http://www.usatoday.com/money/world/2007-07-23-china-spy-2_N.htm?csp=34), last accessed: 24 JUL 2007

## Characteristics of Secure Audit Logging - **How Do I Know I Can Trust My Audit Log?**

Secure audit logging and transactional integrity means more than simply encrypting the log data or simply hashing the log file. Data can be changed and re-encrypted or re-hashed without any obvious detection thereby defeating the purpose of audit logging. Clearly, *more* is needed than simply *maintaining data integrity* of audit logs, such as implemented by solutions that only provide cryptographic hashing of data at a particular moment-in-time. Such approaches are inherently weak because they only provide a moment-in-time snapshot or cryptographic ‘thumbprint’ that cannot detect the combination of unauthorized modification along with a subsequent re-hashing of data files. For example, a privileged user, such as a systems administrator, can commit a fraudulent act and then manipulate audit information to hide her tracks from detection by simply modifying the audit log and re-hashing her records. Since, when using the traditional ‘moment- in-time’ audit log approach, there is no linkage that securely and sequentially binds each log record with time, the evil insider easily has control over the ‘story’ the audit log now tells . Truly a false sense of security could exist in the minds of corporate management if such an inherently weak approach is used as an accountability, forensic or compliance mechanism.

What is needed to provide companies with highly trustworthy audit log data is an approach to securing critical audit log data and electronic transactions from any data source, from the moment it is created and all throughout its lifecycle. Securing such data means that any attempts to modify the data must become evident, rendering the data tamper-evident. Further, any attempt to modify the data, once it is recorded, must be guaranteed to fail, rendering the data tamper-proof. It is only by ensuring that critical audit log and electronic transaction data is absolutely not subject to change, immutable, can such audit data be systematically relied on to accurately

account for the actions taken by even the most privileged users, such as administrators and critical applications. Encryption combined with secure hashing technique, which binds time and record sequence, are two primary technologies used to provide high assurance of the integrity of audit logging. If an attempt is made to breach the security of information protected using these technologies the event becomes highly detectable and easily prevented.

## Business Applications/Databases - Secure Audit Integration

Even the potential of damage due to not being able to effectively prevent, detect and prove unauthorized access and misuse of critical information has moved companies to increase the level of trustworthiness of existing audit and

Benefits that companies have experienced include the increased confidence to embrace new collaborative business models which extend increasing needed access to databases and critical business applications

logging architectures of the systems that companies rely on to run their business. Recent technology advances in the area of secure audit logging and transactional integrity have resulted in highly scalable, centralized source of secure audit trails that can prevent and detect accidental and malicious data alteration. Benefits that companies

have experienced include the increased confidence to embrace new collaborative business models which extend increasing needed access to databases and critical business applications to not only internal employees, but also increased relationship building electronic interaction by customers and business partners in the increasingly collaborative world of next generation Internet usage. As a result now being able to have strong accountability mechanisms in place, companies are able to confidently and quickly take advantage of new business opportunities, strengthen customer relationships, drive efficiency in business partnerships, increase operational

efficiency, and reduce compliance risks. Therefore, whether you purchase off the shelf or develop in house databases, business applications, infrastructure devices, or network security components, secure reliable logging and transactional integrity needs to be factored in as criteria for trustworthiness of the solution you choose. Another area that requires vigilance over information integrity and secure audit logging is compliance.

## Compliance- Secure Logging / Transaction Integrity

At the heart of IT-based regulatory compliance is transactional integrity and reliable logging as part of a risk based compliance management strategy.

Compliance is increasingly becoming a key business issue, and while governance is relatively static, compliance is continuing to evolve. Although in many current regulations the specific requirement for secure audit trails is vague and lightly defined, the requirements will become more stringent as interpretations of the regulations become more established due to legal challenges, litigation and evolving security/risk management standards and best practices.

The following is a sampling of regulations that contain relevant logging data integrity guidance. In some areas of compliance there currently is not a lot of specific guidance regarding logging requirements. At the same, time common compliance themes across most regulations revolve around IT governance best practices and frameworks which themselves are being more finely tuned around secure logging and data integrity.

## Compliance

The Sarbanes-Oxley Act (SOX) - SOX was passed in response to a number of major corporate and accounting scandals. Under SOX companies must account for the accuracy and fairness of their financial reporting; and that appropriate controls over financial data be implemented where such controls are found to be lacking

Payment Card Industry Data Security Standard (PCI DSS) – An international industry standard administered by the PCI Council and enforced by the sponsoring credit card

brands which defines a standard baseline level of security to be implemented to protect credit card data.

Graham Leach Bliley Act (GLBA) – U.S. government legislation that mandates the use of appropriate security controls to protect individuals private financial information.

Companies that offer specified financial services must comply with this law.

Personal Information and Electronic Documents Act (PIPEDA) – Canadian privacy law mandating security and accuracy of personal information used by any person or organization involved in a commercial business.

21 CFR Part 11 – A U.S. government law mandating secure electronic records and electronic signatures as substitutes for paper records and handwritten signatures in electronic transactions of businesses that deal with the Food and Drug Administration (FDA). This law applies primarily to the bio medical industry.

Health Information Portability and Accountability Act (HIPAA) – As the name implies, this U.S. government law intends to protect the privacy of electronic patient health information by mandating accountability through use of risk based management approach to implementing appropriate security controls.

E-Discovery / Forensics – Refers to that group of government rules of evidence and forensics best practices that define legally sanctioned evidence handling processes that make electronic records acceptable in a court of law.

## Governance

Control Objectives of Information and related Technology (CoBIT) - Internationally accepted set of guidance materials for IT governance.

Information Technology Infrastructure Library (ITIL) - A cohesive set of IT service best practice guidance drawn from the public and private sectors across the world.

NIST – U.S. government non regulatory agency within the Department of Commerce mandated, in part, to establish information security management and implementation

guidelines in support of both government and commercial organizations

ISO IEC 27002:2005 - Information technology - Security techniques - Code of practice for information security management - An internationally accepted standard of good practice for information security. This ISO standard establishes guidelines and general principles for initiating, implementing, maintaining, and improving information security management in an organization.

## Conclusion

What is the additional risk of not having secure audit logs and transactional integrity? Failure to assure minimum necessary data disclosure will not only have financial repercussions, but will be a public relations nightmare as well. Secure audit trails, as part of an overall business strategy, help to demonstrate to customers, business partners and regulators that your organization has made a thorough effort to intercept potential problems before they occur by implementing a defensible risk management strategy.

Customer relationships are built on trust and are strengthened by business process transparency. Transactional integrity assured by secure audit trails, cryptographically strong techniques that ensure immutability of logs that document critical business activity, allow your organization to confidently embrace new business opportunities in a fast changing business environment with the knowledge that your company's all important reputation, business processes and competitive advantage are efficiently protected allowing you to minimize avoidable business distraction of security breaches due to strong transactional integrity that secure and reliable audit trails provide to your organization's most critical assets.

What are your answers to these questions?

- Can your audit logs stand up to legal scrutiny?
- Can your audit logs be modified? Can you detect a modification attempt?
- How confident are you in the accuracy and reliability of your audit logs?
- Do you trust your audit logs to definitively prove transactional integrity and accountability?

Secure audit trails provide transactional integrity while reducing your risk and



lowering your compliance costs.

The following cases illustrate the impact of not having in place proper controls and auditing procedures of company critical information.

### **Lack of adequate Audit Logs Means Large Retailer Faces Uncertain Future**

Huge gaps between the originally stated estimates and later estimates of damages, and thus liability, the company must be held accountable for was attributed to inadequate audit logs. The gap in number of compromised credit card accounts ranged between 46 million and 94 million according to court filings from a group of banks that are suing TJX, an off-price retailer of apparel and home fashions. Avivah Litan, a VP and research director at Gartner. "The truth is, forensics is more of an art than a science...it depends on how good the investigator is and what they find." The gap in the estimates also indicates that TJX didn't have adequate audit logs to conduct a proper analysis, she adds. <sup>4</sup>

### **Enron CFO**

Mr. Fastow, the Chief Financial Officer and other members of the Enron executive team made it a habit engaging in time-based data manipulation, i.e., to alter or change financial data to suit whatever it was they wanted the investing public, or governmental authorities to know, or not know. Mr. Fastow has pleaded guilty and is now a guest of the federal government.

### **Next-Card Auditors**

Now defunct NextCard was the largest issuer of Internet MasterCard and Visa credit

---

<sup>4</sup> **Analysis: TJX Breach Doubles; What Difference Does It Make?**, online at: [http://www2.csoonline.com/blog\\_view.html?CID=33250](http://www2.csoonline.com/blog_view.html?CID=33250)

cards. Executives of this former high-flying public company fraudulently and illegally re-characterized loan losses, thereby reducing the amount of cash reserves required. Assisting in no small way in this billion dollar flameout, auditors from Ernst & Young perpetuated the company's fraud by backdating their work papers and their final reports to conform to the fraudulent representations by company executives. These auditors are also currently guests of the federal government. The SEC attorney investigating this matter lamented that the real crime here was that there was no way to ascertain or recover the real, or the true data, because of the time-based data manipulation of these insiders.

### **Parmalat CEO, CFO and Family Members**

In this 18 billion dollar 2003 bankruptcy, the entire CxO level of this multi-national conglomerate engaged in time-based data manipulation by creating an authentic appearing confirmation by Bank of America, on Bank of America Letterhead, and signed by a Bank of America Vice President, to the effect that there existed an offshore bank account holding 5 billion euro on account. In reality both the funds and the account were non-existent, and the alleged Bank of America letter used by the Company to raise billions in the public credit market was pieced together by the company executives using a scanner and Adobe Photoshop, from three totally unrelated sources. The signature of the Bank of America VP was from the information technology department. There are currently at least three lawsuits, including two class actions, pending in various courts around the world.

© Kinamik Data Integrity, 2007

For further information about Kinamik Data Integrity, please contact

[info@kinamik.com](mailto:info@kinamik.com) or visit <http://www.kinamik.com>

