

BAROUDI BLOOR

Audit the Data – or Else.

*Un-audited Data Access Puts
Business at High Risk*

“Accountability is Everything.”

“Creating a comprehensive, perpetual audit hardens an organization against many kinds of loss that often go undetected until it’s too late.”

Introduction

From one perspective, a business is only its data – its customer data, its employee data, its product data, its financial data. Even its processes and partners are represented by data. Compromise the data and you compromise the business. It’s that simple.

In a world replete with regulations and threats, organizations have to go well beyond securing their data. Essentially, they have to perpetually monitor their data in order to know who or what did exactly what, when and how – to all their data. The stakes are high and accountability is everything.

Proving accountability requires not only that all data be monitored. It requires that complete records of access and use be kept. Those records create the audit trail. It is the audit trail that *shows* who did what to what, when and how. It is the audit trail that will snare the villain, detect anomalies, prove compliance and provide assurance that data is used only in intended and appropriate ways. Creating a comprehensive, perpetual audit hardens an organization against many kinds of loss that often go undetected until it’s too late.

Accountability and its instantiation – audit – need to be integral to systems and process design. Baroudi Bloor believes that in time they will be. Just now, however, we as an industry, have a rather large mess on our hands, and need to take concrete steps to address it today.

One significant problem is that organizations and their data, tools and processes came into existence before the demand for audit became acute. We’re trying to apply after the fact functionality that ideally would have been part of the design. To this end, we need to understand that there are better and worse ways to try to solve this problem. In this paper we discuss the hazards that surround data, show the role of audit in mitigating those risks, and describe best practices in auditing data. In addition, we give one example of an intelligent approach to data audit – Lumigent Entegra for Data Audit.

Data At Risk

Businesses are completely dependent on their data. It is a critical corporate asset and needs to be treated that way. Customers, stakeholders and regulators hold businesses accountable for their data and the onus of accountability has fallen on IT.

We've known that data is critical to our business for a long time. If we don't protect salary information, we'll have organizational mutiny. If we don't protect our customer data, we expose ourselves to our competitors and to customer defection. If we don't protect our financial data, we risk theft and fraud. And now, if we don't protect our data, we risk the consequences of not complying with data-protection legislation. Yet every area of vulnerability has grown dramatically with the introduction of Internet technologies – both within and without the organization. Think about the following:

Data Deluge

New data is growing at an average compound rate of about 30 percent per annum, doubling about every 3 years – with some organizations *already* managing terabyte size databases. Any concerns we had about our data a few years ago pale against the concerns we have today, and are trivial compared with what's to come. There's no evidence that suggests we'll have to manage less data in the future. The sheer volume of data is a risk factor – how do you tell if one tiny bit has been compromised?

Digital Under Attack

The rate of IT security breaches continues to increase. A 2002 FBI study, entitled *Computer Crime and Security Survey*, reported that 85 percent of survey respondents had detected security breaches in 2001, with two thirds claiming that they lost money as a consequence. Figures for 2003 from CERT (Computer Emergency Response Team) based at Carnegie Mellon, indicate that the number of incidents almost doubled again in 2003 (www.cert.org has more detailed information). *These figures reflect only those attacks that were detected and reported.* Many attacks go undetected. They are often sophisticated automated techniques for gaining access to systems.

The potential damage to an organization caused by digital intruders varies. At minimum, it demands IT staff time to repair systems and close whatever security loophole was exploited, on top of the lost productivity of anyone affected by the breach. But the major, high-risk damage includes direct financial loss from the destruction of data or its theft, or from fraud. The CSI/FBI statistics for 2002 put the average cost per incident of data theft at \$2.7 million. Other high costs come from brand damage, customer loss, and regulatory penalties.

Digital Fraud

Most digital attacks originate from inside an organization. According to PwC's Economic Crime Survey, 60% of all fraud involves an employee of an organization, often working in collusion with outsiders. The worst cases of digital fraud normally occur from within – employees often have direct knowledge of how systems work, legitimate access to these systems and an understanding of how to exploit them for fraudulent purposes.

Digital fraud is not always a matter of illicit access to systems. It can be the abuse of normal applications: Legitimate staff can change a ship-to address prior to delivery and change it back once they receive the illicit goods. With access to a payroll system, salaries paid to employees that have left the company can be redirected to someone else's direct deposit account.

“The worst cases of digital fraud normally occur from within – employees often have direct knowledge of how systems work, legitimate access to these systems and an understanding of how to exploit them for fraudulent purposes.”

“an avalanche of legislation in the U.S. and worldwide now demands that organizations take responsibility not only for their business data, but for the personal data of their customers and employees as well.”

Human Error, Data Loss, Data Corruption

Various studies indicate that only about 5 percent of catastrophic data loss has a natural or otherwise unavoidable cause. Most data loss and corruption is caused by human error. A study by California-based Broadcasters Network International (BNI) found that 88 percent of the 300 systems managers they surveyed believe accidental deletions cause the bulk of their data-loss headaches. Accidental data loss as well as data loss and corruption as a result of viruses, worms and other malicious acts is on the rise.

Complete data loss is usually lethal to an organization. The University of Texas Center for Research on Information Systems found that 50 percent of companies that lose their data in a disaster never reopen. Ninety percent of the rest go out of business within 2 years of the event.

The cost of any significant data loss is high. Consider the case of the city of Oakland worker who accidentally deleted 15 years of records of CAD/CAM files, irretrievably. Systems that don't have any audit capability flirt with disaster daily. Accidental deletes happen every day and usually go undetected until it is too late to take remedial action.

Input errors can have dire implications as well. Buy.com discovered this in 1999 when it inadvertently offered a \$588 Hitachi monitor for \$164.50 – presumably the person entering the web site data made a mistake. That “input error” ultimately cost Buy.com \$575,000 when they settled the suit filed by the 7000 customers who demanded that Buy.com deliver on its advertised price.

Faulty software can cause data errors and loss as well. For example, if a discounting algorithm has been coded incorrectly, and the discount gets applied twice under certain conditions, the error might go unnoticed for a long time – how many customers complain that they paid too little? Once discovered, it's often impossible to undo the damage that's been done.

Contending with Compliance

In the name of accountability (and culpability) an avalanche of legislation in the U.S. and worldwide now demands that organizations take responsibility not only for their business data, but for the personal data of their customers and employees as well. U.S. data protection legislation includes Sarbanes-Oxley, HIPAA, USA PATRIOT Act, California Senate Bill 1386 and Gramm-Leach-Bliley. Most developed countries, including the EU, Canada, Australia, and others, have also enacted Data Protection legislation. In the banking industry, the New Basel Capital Accord (Basel II) is likely to be adopted worldwide. Financial institutions are subject to regulation by myriad bodies, including the SEC, FRB, FDIC, OTS, NCUA, and various state agencies.

In an ideal world, complete data integrity would mean being able to show that data has not and could not have been compromised. Proving integrity implies providing a comprehensive data audit. Increasingly, legislation requires businesses to audit data access and report events in which that data has been compromised.

The business that does not comply with compliance regulation puts itself at further risk. Business executives who try to mitigate risk by tasking IT with the responsibility for data may find themselves held personally culpable should undetected errors result in the use of inaccurate information or in the unauthorized release of data that should be secured.

Implementing compliance may ultimately benefit everyone – but as the first generation charged with its implementation, companies are finding that compliance can carry a heavy price tag. Failure to prove compliance may prove even costlier. Consider the following legislation and the failure to comply:

The Sarbanes-Oxley Act (SBA) makes the CEO and CFO of a publicly held company personally responsible for his or her company's financial reports. Under SBA, financial misrepresentation is punishable by fines, imprisonment or both, regardless of intent.

To understand the risk of inadequate data protection consider the situation where a database administrator makes a change to information held in financial tables. The change alters some of the financial values that feed into the company's annual financial returns, indicating a slightly better financial situation than was actually the case. Unaware that the figures are misleading the CFO attests to their accuracy. Whether the change was an unintended error or an attempt to manipulate stock values, once the error is discovered the accounts have to be restated and the company stands accused of misleading the market. The event will be damaging to the company's reputation and may involve the CFO in criminal proceedings.

Because of SBA, best practices in accounting now demand the assessment and monitoring of data security, integrity and availability.

California Senate Bill 1386 demands that all organizations provide Californians with immediate notification when confidential information about them has been compromised due to a breach of security on any computer system that stores their personal data. This law applies worldwide to any company holding information on Californian residents.

If a company doing business with California residents is hacked, and that company cannot prove that customer information was not compromised, according to California Senate Bill 1386, that company must alert every one of its California customers. The direct cost alone would be substantial – but the damage to the brand could prove catastrophic. Customers choose where they do business. When doing business means disclosing personal data, the customer is entrusting the business with that data. The company is securing that trust with a promise – that is – the promise of brand. Renege on the promise – forfeit your brand. Forfeit your brand and you forfeit your business. Not a pretty picture.

The Health Insurance Portability and Accountability Act (HIPAA) protects a patient's personally identifiable health information. HIPAA applies to all medical providers who collect protected health information, and carries financial and criminal penalties for any violation, deliberate or otherwise.

Consider the situation where stories circulate in gossip columns about a film star suffering from an embarrassing medical condition. Suspicion will naturally fall on the star's healthcare providers. If these providers cannot prove that there has been no unauthorized viewing of the patient's records, the onus will fall on them.

“....companies are finding that compliance can carry a heavy price tag. Failure to prove compliance may prove even costlier.”

“data audit provides invaluable protection inside an organization – where an organization is most vulnerable.”

“data audit provides the last line of defense for data protection.”

The Gramm-Leach-Bliley ACT (GLBA) and **Basel II** target the financial sector. GLBA protects the confidentiality of personal financial information collected by banks, insurance companies, brokerages and other financial institutions. Beyond GLBA, the banking sector will likely adopt the New Basel Capital Accord, Basel II, which defines banking process aimed at internal control, risk management and assurance.

Most large banks are already starting to move towards compliance with Basel II, which directly impacts IT, requiring that IT departments ensure that the information held in their systems is accurate.

Data accountability is the focus of many other initiatives around the world, including **SEC** audits, **Homeland Security** and the **ISO17799 Code of Practice for Information Security Management**. As initiatives are adopted, companies that don't comply risk substantial legal (and financial) liability.

Another impetus for auditing data activity is the need for best practices, which are required by Federal Sentencing Guidelines, insurers, audit guidelines, and common sense.

Mitigating the Risk to Data through Audit

Data – we can't live without it, and living with it puts us at risk. Baroudi Bloor believes that implementing a comprehensive data audit can largely mitigate that risk. Data audit enables an organization to identify who created, changed, deleted or accessed data – when and how. The very existence of data audit can have a strong chill affect on would-be perpetrators – no action would go unseen.

Including an alert capability to draw attention to anomalous data events means that problems surface quickly with a much greater probability of timely, effective resolution. When problems aren't found for 18 months, which is typical with digital fraud, for example, the likelihood of apprehending the thief plummets. Further, the audit trail provides important prosecuting evidence.

Data audit should be an integral part of operations. Not only does it augment rigorous perimeter security by actively logging all access to all data, **data audit provides invaluable protection inside an organization – where an organization is most vulnerable**.

Groan as we may, regulation is a growing part of our business existence. **Data audit can provide a coherent framework for compliance mandates**, ensuring that data are appropriately monitored and that breaches are reported. Adding data audit to strong policy management and other forms of IT security protects an organization much more thoroughly than do policy and security alone. Providing a complete record of data access, changes to data, and changes to database structure such as logins and permissions, data audit enables organizations to verify and demonstrate adherence to security policies and compliance imperatives. Because of the shifting sands of requirements and capabilities, policies and technical safeguards are often flawed the moment they are implemented – data audit provides the last line of defense for data protection.

Some **compliance may bring business benefits in its own right**, somewhat assuaging the inherent pain. For example, complying with Basel II is potentially advantageous for banking institutions. Banks that can demonstrate an advanced level of risk management will reduce their capital and long-term costs by virtue of being a better credit risk. In general, compliance to regulatory mandates makes it easier for businesses to do business with other businesses – companies are more willing to partner with businesses they know to be secure.

A data audit capability can greatly enhance the operational integrity.

Audit trails show complete details of all structural changes and transactions and their consequences, making recovery from accidental deletion or erroneous data entry relatively simple.

Automating data audit process saves money. As the need for audit continues to increase, the cost of manual audit increases as well. Automating data audit is ultimately much more effective and efficient – data audit is an always-on process that needs to extend and adapt to reflect changes in an organization. Fully vetted automated audit is much less prone to human error, much more scalable and manageable, and much less susceptible to compromise.

Best Practices for Data Auditing

Making an organization completely accountable for all its data can seem a mammoth task. Despite increased sophistication in every area of computing, we have no built-in, comprehensive and dependable mechanisms that provide a bulletproof audit trail showing how data has been accessed or used. Continuously auditing existing systems and processes is a huge undertaking – one that requires in-depth analysis, courage and follow-through. It is not a task for the feint of heart. Yet every business that wants to stay in business must address it – and the sooner the better. For most, it's evolutionary.

We've gathered what we believe are best practices in auditing. Like any set of best practices, we mean it to be extensible. If you identify other important elements, please let us know. Here's what we've identified:

Separate Responsibility. The team responsible for auditing a system must be distinct from the team that's administering and using that system. There must be no possible conflict of interest. It's particularly important to separate audit from other aspects of IT such as database administration. This "separation of duty" is a key principle of auditing frameworks used to evaluate compliance.

Keep the Data Audit System Independent. The data audit system needs to be independent of other IT systems, (with the possible exception of other IT security systems). All data audit information must be restricted to read-only access. Nothing or no one should be able to alter an audit trail.

Make it Scalable, Extensible, Efficient. The data-auditing platform must accommodate growth and the addition of new data resources. Keep its operation overhead low, so that extending or scaling its use is cost effective. From an operational perspective, data audit is an integral part of the applications environment.

Make it Flexible. Audit requirements will change – ensure that you can respond quickly and easily to those changes by deploying a flexible audit framework.

Centralize Management. Ensure that operational procedures are controlled from a single point and that analytics can be applied to the whole data audit record. A data-auditing platform must be capable of auditing multiple databases on multiple physical servers.

“Automating data audit is ultimately much more effective and efficient – data audit is an always-on process that needs to extend and adapt to reflect changes in an organization.”

“All usage must be closely controlled and audited, maintaining a complete record of who accessed information in any way.”

Secure the Data Audit Platform. The security of the data audit capability must be guaranteed so as to prevent any interference with its operation in any way by staff other than those designated. It must not be possible to turn it off, except by the staff administering it. A record of all times that it goes out of service for any reason must be kept. The data audit platform itself must contain no “back door access” to its own data or allow such back door access to the data of any of the databases it monitors.

Identify the Data. Establish and maintain an inventory of all data, including data coming from outside sources.

Analyze the Data. Determine the roles, vulnerabilities and liabilities relative to all data. Assess the data from an operational perspective, as a target for fraud, and from a compliance perspective.

Make it Complete. Ultimately, data audit policy needs to embrace all data in an organization, including all application data, all communications data including e-mail and instant message logs, transaction log files and all information passed to or around an organization from the inside or outside.

The data audit must create a complete record of who accesses data when and through what application or utility. Where data changes occur, before and after values must be recorded. The audit must record all database design changes, all schema changes, all changes to access permissions, and any data access through database utilities. The audit must record who accessed the data, when and via what path. Any access path not under the purview of the audit must be closed.

Enable Reporting and Analytics. To use data audit forensically – that is, to determine what happened – requires the ability to view data broadly and in-detail. It must be possible to assess any impact on data from the beginning to end of any transaction.

Establish Normal Usage Patterns. Without normal usage patterns, it’s difficult to detect anomalous usage.

Establish, Document and Review Policy. Create policy to govern the use of the data audit capability and review it regularly in light of regulatory and compliance demands, organizational changes, new applications, partnerships or interactions. Where data is shared with other organizations or comes from other organizations, the data audit policy for that data must be agreed between organizations, with responsibilities contractually defined. Understand that an organization cannot outsource its risk along with its data.

Documenting data audit usage is critical and becomes part of the audit process itself. This documentation articulates the audit process and is necessary both for forensic and compliance issues. Data audit implemented directly to satisfy regulatory mandate should refer directly to the elements of the regulations it satisfies (Sarbanes-Oxley, HIPAA, GLBA, etc.).

Various constituencies within an organization have legitimate reasons to track the use of data. All usage must be closely controlled and audited, maintaining a complete record of who accessed information in any way.

Monitor, Alert, Report. Depending on the risk, tie anomalous events or data to alert systems – potentially real-time alarms.

Augment and Complement Security. Data Audit augments and complements other IT security – particularly perimeter security (firewalls, IDS, encryption, etc.) and identity management. Data audit mitigates the risk inside the firewall – where, in fact, data is at greater risk. For the audit to be reliable, user identities must be secure and properly managed. All changes to identity and access permissions, both for applications and databases, must be audited.

Back up and Archive. The data audit trail is critical to an organization's operations and security. The audit trail itself must be backed up, archived, and, ideally, stored remotely.

Create Procedures for Operational and Disaster Recovery. The audit trail is where everyone will turn when there's data loss or compromise of any kind. Create policies and procedures that govern how the audit trail is accessed and how to recover loss. All recovery operations must be audited as well.

Creating the Data Audit

Most businesses have policies and procedures in place that reduce risk to data. However, few companies have implemented any kind of audit trail for data, and, of those, most use database triggers or modify their applications, which increases risk rather than reducing it.

Database triggers are difficult to create and deploy, require perpetual management and impact overall performance. Their administration is typically under the purview of the database administrator – undermining the essential need for independence in audit. They typically cannot capture data access activity.

Modifying applications is a dangerous and unending task. Each and every application has to be modified in every place at which data activity may occur. The modifications themselves introduce risk. The process is costly and labor-intensive and far from foolproof. Applications that were purchased as product may not allow modification – or modifying them could render them unsupported by the application vendor. When the application needs to be patched or revved, the audit modification might have to be done over from scratch. Modifying the applications does not address someone directly accessing the database itself.

Both of these approaches rely on the integrity and competence of the developers tasked with design and implementation. Do these developers completely and thoroughly understand every possible nuance and scenario now and in the future to the extent that they can ensure a failsafe audit? Are they beyond leaving some back door in for “operational use only”?

Neither creating database triggers nor modifying applications provide what's needed for real data accountability. Neither of these approaches captures changes to database permissions and schema – an easy way to subvert simplistic approaches to audit. Neither provides the independence needed for reliable audit.

“few companies have implemented any kind of audit trail for data, and, of those, most use database triggers or modify their applications, which increases risk rather than reducing it.”

“Lumigent’s approach to data audit reflects a deep understanding of both the risks inherent in data and the benefits of providing comprehensive data audit.”

A Platform for Enterprise Data Audit: Lumigent® Entegra™

Lumigent has taken a very different approach, creating a data audit capability that operates independently of other systems. This independence is critical for gaining irrefutable information – for true data forensics, complete operational integrity and actual compliance verification. Lumigent’s data audit products operate independently of both other applications and database administration. It is outside both the applications and the data, monitoring all access to all systems to create a comprehensive view and end-to-end audit.

Lumigent Entegra software directly interfaces with database management systems. Entegra uses three different agents to monitor and collect data from databases: *a data modification agent* that monitors and records all modifications within the database, *a data view agent* that reports all access to data held in the database, and *a structure agent* that monitors structural, permissions, and login activity. An *alerting capability* generates alerts of suspicious or unusual activity in the database.

Entegra captures database activities directly, and records the SQL access statements, user details, date and time and session information, and changes to data when they are made. The data activity from multiple servers is consolidated into a unified, structured repository and can be viewed using standard reporting tools, but Entegra also provides a report server that includes browser access, including filtering features that can customize display results for different users. Audit data can be archived regularly to make room for new data. Administration and deployment from a single console provides easy management.

In Conclusion

Businesses have a responsibility to their shareholders, business partners, customers, regulators, auditors and staff for the responsible management of data. Unauthorized access or unintended changes to an organization’s data can cripple or ruin a business. Data theft, error, loss, corruption or fraud can cost a company its reputation, its profits, or both. Data audit not only protects an organization’s data, it ensures accountability, recovery and longevity for an organization’s data-dependent systems.

A comprehensive data audit capability delivers operational benefits beyond risk management and reduction, and legislative compliance. It complements the whole range of IT security, improves the operational integrity of overall IT systems, establishes accountability for data usage across an enterprise, and provides a means to analyze data usage.

As an industry, we have yet to design audit and accountability into our systems. Baroudi Bloor believes that Lumigent’s approach to data audit reflects a deep understanding of both the risks inherent in data and the benefits of providing comprehensive data audit. Lumigent’s independent and comprehensive approach has the potential to significantly mitigate data risk across the spectrum of threat – from internal and external attack, human error, and natural disaster to regulatory compliance. Lumigent’s approach is sane, sensible and extensible and can give organizations the assurance that their single greatest corporate asset – their data – is truly protected.

This white paper was written by Robin Bloor and Carol Baroudi of Baroudi Bloor International Inc. for Lumigent Inc. to position Lumigent's Entegra technology. Baroudi Bloor International is a research, analysis and strategic advisory company serving high technology vendors and users.

Robin Bloor is Research Director of Baroudi Bloor International, and President of Bloor Research, one of the world's leading IT analyst and consultancy organizations distributing research and analysis to IT user and vendor organizations throughout the world. Contact him at robin@baroudi.com.

*Carol Baroudi is CEO and founder of Baroudi Bloor. Her more than 20 years of IT industry experience include VP, Emerging Technologies, at Hurwitz Group, and co-authoring the best-selling Internet book of all time – *The Internet For Dummies*, and an earlier background in information architecture, management consulting and software development. Contact her at carol@baroudi.com.*



BAROUDI BLOOR

175 Pleasant Street ◀ Arlington, MA 02476 ▶ 617-747-4045 ▶ www.baroudi.com