



NETFORENSICS WHITE PAPER

Think Data Breaches Can't Happen To You? Think Again.

A Look Into Recent Breaches and
How to Defend Against Them

The Current State of Affairs

Corporations and consumers alike experienced an intense economic climate in 2008. Fraught with threats to global financial markets and personal financial security, companies and individuals were dealt additional blows when several of the largest data breaches in history occurred. Firewalls were penetrated, networks were hacked, malware infiltrated servers and web applications, and confidential records were compromised. Companies like Countrywide Financial Corp., TJX Companies, and the Bank of New York Mellon — and especially their customers — experienced the painful challenges of data exposure. So did many other companies. According to the Identity Theft Resource Center (ITRC) of San Diego, businesses, governments, and educational institutions reported nearly 50 percent more data breaches in 2008 than in 2007. The ITRC reports that 327 data breaches occurred in 2008, exposing 13,203,031 records⁽¹⁾.

Regardless of the level of sophistication and aggressiveness of these attacks, companies failed to detect breaches when they occurred. Yet high-profile, damaging data breaches are nothing new, and they have sparked many companies in recent years to employ more intelligent, proactive information security measures within their organizations. At the same time, regulatory compliance demands continue to intensify across industries, putting companies under additional pressure to better protect valuable, confidential data. **So why are these data breaches still occurring in such alarming numbers with often devastating consequences to companies and consumers?**



In some breaches, the root cause is clear, such as a stolen laptop or employee negligence. In other cases, it takes an intense investigation to determine what happened and how. Recently, the Verizon Business RISK Team, a world-renowned data forensics organization, investigated suspected breaches occurring from 2004 to 2008, presenting detailed firsthand evidence in their report, 2009 Data Breach Investigations Report. The results are enlightening and offer companies reason to revisit their security strategies. According to Verizon, "The majority of breaches still occur because basic controls were not in place or because those that were present were not consistently implemented across the organization ⁽²⁾." They add, "Most of these incidents do not require difficult or expensive preventive controls; mistakes and oversight hinder security efforts more than a lack of resources." Yet more often, the opportunity for detection is there. Investigators noted that "66 percent of victims had sufficient evidence available within their logs to discover the breach had they been more diligent in analyzing such resources."

In essence, simply collecting event data through log management — though important and almost always required by compliance mandates — is not enough to secure the enterprise. Companies must expand their log management efforts to include in-depth visibility into logs across the company. This requires correlating the logs for a complete and clear understanding of events, patterns, and trends in real time, so organizations can stop the attacks before they reach important data. Security information management (SIM) solutions together with log management tools can provide companies with the insight needed to successfully protect important business data and ensure a secure environment.



Recent Data Breaches: A Closer Look

Whether they inflict their pain on a well-known, global corporation or an unassuming small, local business, data breaches can impact companies and their customers in many unsavory ways — from creating inconveniences for network administration teams, to exposing personal information to theft, to causing long-term damage to businesses. Consumer accounts are hacked and huge sums of money disappear. Personal identities are stolen. Consumer trust in targeted companies dwindles, causing profits to fall. Organizations must dedicate funds, sometimes in the millions of dollars, on reporting data breaches to any customers potentially exposed.

While data breaches continue to impact businesses and consumers, a close look at individual breaches—what exactly occurred and how the company could have prevented it —can offer valuable insight for any organization wanting to strengthen its security posture and prevent a similar data breach from occurring. The following recent and costly security incidents illustrate how corporate data is being compromised and what companies can do in an effort to prevent these breaches from happening to them.

University of Florida

Breach – In November 2008, the University of Florida College of Dentistry in Gainesville fell victim to an aggressive hacker. Approximately 330,000 social security numbers were exposed during the breach. Onsite system administrators noted that prior to the event the university had implemented new controls and measures for securing information on its servers and systems. They strengthened firewalls and intrusion detection systems, encrypted data flows containing sensitive information, and stepped up procedures for identifying threats and security servers. Nonetheless, valuable data was exposed.

Prevention – Though the University of Florida made a concerted effort to protect its data, the security breach proves they had not done enough. Attacks to the databases failed to alert management and IT personnel, even while they had tools in place to collect log

event data day after day. As anomalies in behavioral patterns occurred, they went unreported and therefore unnoticed. Why? It appears that the university had taken individual precautions, such as logging and firewalls, yet they lacked the tools and processes to integrate the information for end-to-end visibility into what was taking place. They needed better real-time correlation of security event logs to expose the necessary details and tie them all together, while they were occurring. By correlating database logs, firewall logs and events, intrusion detection system logs, system access logs, and so forth, they could have better understood what was happening and the relationship among activities, uncovering the unusual security events taking place.

U.S. Electrical Grid

Breach –Electrical grids in the U.S. provide the infrastructure for our electric power. In April 2009, hackers broke into the U.S. electrical grid systems and installed control programs on these systems, putting electrical service and government infrastructure at risk. Left undetected, these programs could have severely disrupted major components of the electrical grid. Though the hackers failed to succeed in impacting electrical service, the fact that they penetrated the critical infrastructure causes great alarm.

Prevention – Given the sensitivity of these kinds of events, few details were made public. Yet certainly, systems were not talking to one another and security event data properly correlated could have prevented the attacks. Somewhere along the way, vulnerabilities existed — in a platform or an application and eventually the power control systems—even with firewalls, intrusion detection systems, and logging devices in place. Visibility through real-time correlation would have tied together individual events in the firewalls, applications, and systems, for example, exposed the chain of events occurring, and then triggered the necessary alarms due to the resulting and suspicious patterns.



U.S. Joint Strike Fighter Program

Breach – The U.S. Joint Strike Fighter Program is the U.S. Department of Defense's focal point for defining strike aircraft weapon systems for the Navy, Air Force, Marines, and U.S. allies. In April 2009, intruders entered and compromised systems via multiple defense contactor networks, including Lockheed Martin and Northrop Grumman sites. Large quantities of sensitive data were successfully downloaded, and data was automatically encrypted as it was accessed and retrieved, making it difficult to determine what data was leaked.

Prevention – Certainly, contractors affected had a logging infrastructure and systems in place to detect intrusions, yet apparently their efforts were insufficient. Interestingly, the Verizon report revealed that 69 percent of the data breaches reported were discovered by a third party, including vendors, suppliers, contractors, and customers. A closer watch on the extended enterprise is critical, especially for military organizations.

University of California at Berkeley

Breach – In May 2009, overseas hackers accessed Web-accessible databases at the University of California at Berkeley containing 160,000 student records that included health insurance data and social security numbers. Astonishingly, the hacks, probably SQL injection attacks, began in October 2008 and continued for seven months. Eventually, a system administrator happened to notice messages left behind by the attackers, exposing the data breach. Upon investigation, the university traced the IP addresses back to Asia.

Prevention – These ongoing attacks could have been mitigated with a comprehensive approach to security that told the whole story. Correlated database event logs, Web application logs, firewall logs, system logs, and account access logs could have revealed anomalies and intrusions from the onset.



Why the Rise in Data Breaches?

The Verizon 2009 Data Breach Investigation Report offers important insight into the patterns and prevalence of recent data breaches. The Verizon team investigating 90 confirmed breaches, most occurring in 2008, revealed an astounding 285 million records compromised. **Key findings from the report include:**

- **74 percent of the incidents originated from outside sources**
- **64 percent of the breaches resulted from hacking, comprising 94 percent of records compromised**
- **83 percent of the breaches were not highly difficult to achieve**
Approximately 80 percent of the breaches appeared in the firewall logs
- **In 75 percent of the cases, breaches went undiscovered and uncontained for weeks or months**
- **Attacks are moving up the computing structure to the application layer**
- **Even with good log management, breaches are still occurring**
- **The utilization of detective controls among breach victims is relatively low**
- **Data thieves seem to show no partiality between larger enterprises and smaller establishments; criminals typically initiate attacks based on perceived value of the data and convenience**
- **Mistakes and oversight hinder security efforts more than a lack of resources**
- **Most of these incidents do not require difficult or expensive preventive controls; 87 percent were considered avoidable through the implementation of simple or intermediate controls**

Clearly, cyber attackers and their techniques continue to evolve, yet many companies are not keeping pace with the growing level of sophistication underlying security attacks. Rather than lacking the necessary resources to sufficiently protect their corporate data, they often lack the right tools and processes to adequately analyze events as they are happening. The security data exists in their organization, yet they have not figured out how to leverage it to prevent and mitigate risk. As noted by Verizon, “All too often, evidence of events leading to breaches was available to the victim but this information was neither noticed nor acted upon. Processes that provide sensible, efficient, and effective monitoring and response are critical to protecting data.” Importantly, companies need to do more than collect event logs. They must correlate them to identify suspicious patterns in the logs that could indicate an impending attack or inappropriate activity.

Defending Against Threats and Breaches

Organizations must refine their security efforts, as evidenced by the recent increase in security breaches and the resulting compromise of sensitive information. Security intelligence is necessary for prevention, including enterprise-wide visibility into security events — and effective alignment of people, processes, and technology. Organizations should have a standard log-review policy that requires them to review security event data beyond operating system, network, and firewall logs to include databases, Web applications, remote access services, and other critical applications. Yet simple log management products demand that security staffs conduct manual event correlation, making it impossible to have the level of day-to-day understanding about potential breaches and attacks needed to prevent damage. In fact, with basic log management, companies typically find out about these attacks and breaches long after they occur.

Instead, organizations need automated, real-time event correlation, made possible by a combined SIM and log management strategy. To defend against threats and data breaches, companies need a reliable, integrated solution that captures volumes of diverse data from

across the network, centralizes and archives event logs, and provides in-depth reporting. Today's increasingly targeted and hard-to-detect threats require visibility into logs, understanding patterns and trends in real time, and identifying threats as *they happen*.

Real-time correlation is the key, including correlation of:

- **System event data**
- **System access logs**
- **Application logs**
- **Database logs**
- **Network device logs**
- **Intrusion detection system events**
- **Vulnerability assessment data**
- **Performance data**
- **Behavioral data**

When companies have the right correlation capabilities, they can automatically collect massive amounts of security-incident data and zero in on the security events that suggest potential problems. Multiple reporting devices can detect and alert on suspicious redundant activities, such as multiple login failures, that confirm that an event has occurred at a particular point in time. Statistical correlation can search for anomalies by gauging the relative relationship between two or more variables — such as the number of incoming emails versus outgoing emails on a given day, to alert on a spam server installation. Pattern-or rule-based event correlation can allow companies to identify behaviors indicative of attacks through comparing them with a catalog of real-world attack patterns.

Event correlation technologies go beyond simply collecting and storing logs. Rather, they allow companies to be proactive and discover attacks as they occur to enable a rapid response. With a clear view into their security posture at any point in time, organizations can stop attacks in their tracks before real damage occurs. netForensics offers the essential SIM and log management tools to help prevent data breaches from occurring.

Putting Security Logs to Work

netForensics offers the important capabilities needed to ensure adequate protection from security threats including attacks on systems, applications, and databases containing sensitive company data. The nFX SIM One and nFX Cinxi One products, part of the nFX One family of solutions, allow ongoing data collection from network and security devices. More importantly, they offer the capability to normalize, aggregate, and correlate the security data collected. These netForensics solutions provide complete visibility into the security information and enable real-time identification of threats and patterns of suspicious activity, so organizations always know their security and compliance stance.

nFX Cinxi One – nFX Cinxi one offers SIM and log management in a single appliance for organizations of all sizes, and is especially suited for companies with budgetary and resource constraints, such as midsize companies. Cinxi provides a complete view of enterprise security posture and rapidly identifies suspicious patterns of activity that would otherwise go unnoticed. Multiple views of actionable security information are tightly integrated with reporting and analytics to rapidly and intuitively pinpoint the true threats.

nFX SIM One – The nFX SIM One enterprise-class SIM solution transforms volumes of disparate, security-related data into actionable intelligence. The highly scalable SIM One empowers large organizations and managed service providers with complex networks to centrally gather, analyze, and accurately report on security events and risk posture. By identifying and enabling a rapid response to threats and providing an auditable compliance framework, nFX SIM One helps prevent threats and protect valuable data.

Conclusion

Protecting critical assets is getting tougher, as attacks and breaches are becoming increasingly subtle and sophisticated. Though 2008 presented us with numerous well-known, damaging data incidents, data breaches continue to plague organizations in virtually every industry, year after year. When such incidents are discovered, response is critical. Organizations must quickly contain the damage, protect corporate and customer data, discover the root cause, and generate detailed reports of the process.

Log management is an important component to defending against data breaches, yet organizations need more, including the power to investigate log data for suspicious patterns. Companies need to make sense of their logs and tie together activities across the network by combining log management with SIM. Through the combined solution, organizations can conduct ongoing, real-time correlation of security event data, enabling real-time visibility into log data.

netForensics offers a best-practices approach to information security that includes the necessary SIM and log capabilities. In addition to the enterprise-class nFX SIM One product, netForensics offers the industry's first low-cost, integrated security and compliance solution — nFX Cinxi One — with log management and SIM capabilities built into one appliance. With nFX One, companies can move beyond simple log management to real-time correlation of security logs and events, offering the insight needed to successfully defend against data breaches, protect important business data, and ensure a secure environment.

About netForensics

netForensics, the Security Information and Event Management leader, enables organizations of all sizes to rapidly identify and respond to threats and demonstrate compliance. Our solutions deliver real-time security intelligence that is accurate, actionable, logged and easily managed. Award-winning nFX Cinxi One is the industry's only solution that combines security information management (SIM) and log management on one appliance and is recognized for its ease of deployment and management. For over a decade, our nFX SIM One software solution has helped enterprises, managed service providers and government agencies around the world to manage risk, protect their assets, and maintain compliant operations.

References:

- (1) ITRC Breach Report 2009, September 8, 2009 (www.idtheftcenter.org/ITRC_Breach_Report_2009.pdf)
- (2) 2009 Data Breach Investigations Report, Verizon Business RISK Team, Verizon, 2009.