

**"Highest Performance  
Lowest Price"**

**Microsoft**  
GOLD CERTIFIED  
Partner

# **GFI** WHITE PAPER

## **Automated event log management for PCI DSS compliance**

### **A practical approach to effective network security**

This white paper highlights why organizations need to implement event log auditing as an integral part of their security policy to meet industry standards such as the Payment Card Industry Data Security Standard (PCI DSS).



### **Sign up to GFI's FREE SMB-Zone Newsletter**

Receive FREE invites to SMB focused content such as IT Advice,  
Topical White Papers, MVP Tips and Tricks, Webcasts and much more!



# Automated event log management for PCI DSS compliance

## Introduction

At one point or another – like the majority of computer users – you have received emails that promise business deals worth millions of pounds, that try to sell products to improve your appearance or that try to convince that it’s worth investing your money in a particular company or stock. Dealing with spam (unsolicited email that is not targeted at specific individuals), is one problem that all email users share in common. Research shows that between 65% and 90% of all email received is considered spam.

On an individual user basis, spam is annoying; it is a waste of time and often contains spyware, malware and even pornography. On a company-wide basis, the same threats apply however there is also the financial cost to manage spam that must be taken into consideration.

Introduction.....	2
The need for PCI DSS.....	2
PCI DSS and event log auditing: What is the connection? .....	3
Consequences and implications of non-compliance .....	3
The aches and pains of event log management.....	4
The antidote: Automated event log management .....	6
GFI EventsManager.....	6
Conclusion .....	6
About GFI.....	7

## The need for PCI DSS

PCI DSS is a collection of best practice procedures that attempt a drastic reduction of credit card fraud. Its main objective is the setting in motion of a cultural shift towards a more security-centric mentality in all businesses operating within the payment card industry. This need arises from the fact that credit card fraud has skyrocketed in the last few years, leading to an astounding financial loss of \$3028.8 million in the US alone in 2006 (ePaynews.com, 2006). The rise in fraud levels is fuelled by 3 factors:

- The availability and sheer simplicity of e-commerce, which conveniently overcomes geographical boundaries and, often, any protection offered by local laws and regulations.
- The high availability of “plastic money” for consumer purchases in all industrialized nations.
- Substandard security practices implemented by merchants and merchant service providers that store, process and transmit unprotected payment card details without taking precautions against whoever might tap into this information



## Automated event log management for PCI DSS compliance

To counter credit/debit card fraud, the 5 major card companies (Visa International, MasterCard Worldwide, American Express, JCB and Discover Financial Services) designed a strong security framework to reinforce payment card transaction security. The result of their efforts was the Payment Card Industry Data Security Standard (PCI DSS).

PCI DSS compliance is today the irrefutable responsibility of all businesses handling cardholder data including retail, mail orders, telephone orders and e-commerce – irrespective of business size.

### PCI DSS and event log auditing: What is the connection?

Swiping a credit card at a merchant's shop or clicking the 'purchase' button on an e-commerce website triggers a number of background processes (e.g. transaction validation process) – all of which generate event log entries on servers, security applications, hardware components and lots of other places across the network. Similarly, classic computer attacks and hacks such as dictionary and brute force password attacks generate event log entries in the security logs of your IT infrastructure. The meticulous auditing of infrastructural logs therefore makes it possible for security administrators to monitor system usage trends and identify possible foul play.

PCI DSS requirements address event log auditing by explicitly underlining the need to collect, audit and manage event log data. The need for effective event log management goes beyond a single PCI DSS requirement. For example, PCI DSS requirement 10 dictates that all businesses utilizing payment card information should "track and monitor all access to network resources" – a requirement that can be easily achieved through event log auditing. Other PCI DSS specifications, such as requirement 5 demands that companies "use and regularly update anti-virus software", an activity which administrators can also verify through the event log entries generated within the anti-virus event repository.

PCI DSS specifications extend to all network hardware and software components that are used within environments that store, process and transmit credit/debit card data. These include:

- Core network-security components such as firewalls, routers, Intrusion Prevention Systems (IPS) and Intrusion Detection Systems (IDS)
- Network segments such as Demilitarized zones (DMZ)
- Servers and business systems hosting DNS services, NTP services, SMTP/POP3/IMAP and other email services, authentication handling, Active Directory policies, web servers and database servers amongst others
- Internal or web-facing applications including off-the-shelf and custom-built software.

### Consequences and implications of non-compliance

Only companies that take event log management seriously can meet the strict requirements of the PCI DSS. Failing to do so can lead to serious repercussions. Between May 2006 and January 2007, retail giant TJX became a victim of what can be considered to be one of the greatest computer breaches that ever occurred in the payment card industry. Hackers exploited flaws in a segment of TJX's computer network that handles credit and debit cards, checks, and merchandize return transactions to steal over 45 million credit/debit card records. The stolen information was used in various fraudulent card transactions including the Florida crime spree of March



## Automated event log management for PCI DSS compliance

2007. According to various experts, TJX violated some of the basic tenets of PCI DSS and consequently, this retail giant now faces numerous lawsuits that will eventually lead to severe financial sanctions that can amount up to \$500,000 per incident.

Organized crime, however, targets business of all sizes, not just Enterprise or Fortune 500 companies. Speaking at an IT security event at London's House of Lords in November 2006, former White House Security Adviser Howard Schmidt urged that "...small and mid-sized enterprises have to realize that just because they are small, it doesn't mean they won't be targeted. Bad guys target wherever they can get money" ([CNET News.com](http://www.cnet.com)).

That is what happened to Johnny's Selected Seeds, a relatively small seed company with about 100 employees, in Maine, USA. On February 4, 2007, their website was hacked and over 11,500 credit/debit card records were stolen. It took two weeks before administrators got to know about the breach, when two customers called the company claiming that their credit cards had been compromised with fraudulent charges.

Through PCI DSS the PCI Security Standards Council acknowledged that no company is immune to network security breaches. A single compromised system out of many servers, workstations, software applications and network components through which payment card information is relayed, can be the catalyst of a serious network security breach. In view of this, all major card brands are pushing for PCI DSS compliance in all world regions. Hefty fines up to \$500,000 (per incident) are looming for non-compliant level 1 and level 2 merchants that get compromised after the September 30 and December 31, 2007 deadlines respectively. Non-compliant service providers on the other hand are already liable to these fines since their compliance deadlines expired in 2005. In addition, fines up to as much as \$100,000 per incident have also been set for merchants and service providers that fail to disclose payment cardholder data security breaches. For more information related to merchants, service providers, the compliance levels that they have to conform to and how this can be achieved refer to: <http://www.gfi.com/whitepapers/pci-dss-made-easy.pdf>.

### The aches and pains of event log management

With security being as strong as its weakest link, it is of critical importance that foul play is identified in a timely fashion and weaknesses are "plugged" before these are actively exploited. The PCI DSS comprises 12 general requirements designed to:

- Build and maintain a secure network
- Protect (cardholder) data in transit or at rest
- Maintain a vulnerability management program
- Implement strong access control measures
- Regularly monitor and test your IT infrastructure
- Maintain an information security policy.

Event log management plays a fundamental role in meeting these objectives. Significant event logs contain a history of network happenings such as an audit trail that details failed logon attempts, configuration changes in



## Automated event log management for PCI DSS compliance

security/authentication policies and much more. It's through this information that IT professionals can effectively gauge access control measures, verify security safeguards and monitor IT infrastructure activity.

Notwithstanding the fact that event log management is a mandatory process, systems administrators find it to be an extremely daunting task to undertake. All hardware and software components on a corporate network generate events that need to be audited, understood and acted upon. To fulfill this charge, automation is the key that enables IT professionals to overcome challenges such as the following.

**Challenge 1 – Event logs are distributed:** Event logs are located on all workstations, laptops, servers and network devices on a local area network (LAN) or a wide area network (WAN). Consequently, systems administrators have to physically log on to each computer to retrieve event records. This is aggravated when event logs are located across diverse geographical locations where IT professionals often have to rely on non-technical personnel or third parties to retrieve this data.

**Challenge 2 – Oversized event logs obstruct event discovery:** Hundreds of thousands of event log entries are generated by all computers and network devices over LANs and WANs. Managing this extreme volume of events data is time consuming. Furthermore, the lack of event filtering mechanisms that sift out trivial events, commonly referred to as 'noise', makes forensic investigation an intimidating task. Identifying key events buried deep within this sheer volume of log data is as complex as looking for a needle in a haystack! In addition, the large volumes of event-log data require extremely large storage repositories, additional processing power whilst deteriorating event-browsing performance and slowing down report generation.

**Challenge 3 – Default tools and reports are toothless:** The management and reporting tools bundled by default with operating systems and devices that generate logs are limited or inexistent. Systems administrators have, for example, limited event correlation and investigation tools, no granular control over event log searches, no event filters to sift out trivial data and very limited reporting utilities – often too limited to provide the evidence that administrators require to demonstrate systems status and compliancy efforts.

**Challenge 4 – Log diversity encumbers correlation:** Heterogeneous networks generate diverse log types – most commonly Windows events, Syslog and W3C logs. This creates problems for systems administrators who are required to use different event management mechanisms for every log type. This leads to additional overheads such as different solutions to install, manage and maintain, diverse consoles to learn, different ways and features through which event browsing is performed, dissimilar reporting mechanisms – a total lack of the 'common look and feel' philosophy. Additionally, diverse log types generate the need for different event storage repositories.

**Challenge 5 – Cryptic log formats breed complexity:** Event log data is in most cases cryptic and therefore not easily interpreted by administrators. Systems administrators have to acquire considerable technical knowledge or research volumes of technical publications to decipher what event logs are really saying.

**Challenge 6 – Standards compliance erodes precious human and technical resources:** Compliance to industry directives such as PCI DSS is a labor-intensive endeavor that can bring already overstretched IT departments to their knees. With IT professionals struggling to address the granular security requirements imposed by such standards and the fact that companies are deemed guilty until proven innocent, systems administrators have to provide tangible proof that demonstrates they are exacting due diligence efforts. Additionally security is subjective and many companies often live in a false sense of security – ending up facing serious repercussions after an attack or even failing compliance audits.



## Automated event log management for PCI DSS compliance

### The antidote: Automated event log management

Ingenious and forward-thinking corporations achieve success in securing their network and attaining PCI DSS compliance through the adoption of advanced event log management solutions. Businesses identify manual event management as being plagued with the above-mentioned challenges and as being the weakest link in limiting compliance efforts. Event log auditing challenges are resolved by deploying a solution which:

- Automatically collects event logs from distributed sources and consolidates them into a central repository.
- Automatically sifts out trivial events – thinning down the events data into a manageable size.
- Incorporates all forensic investigation, log management and reporting mechanisms required to investigate network activity, generate reports and unblinkingly watch over cardholder data 24x7x365 days in compliance with PCI DSS.
- Allows the management of diverse event log types through a single solution that incorporates one management console as well as a common look and feel approach to log processing, browsing, investigation and reporting.
- Decodes cryptic logs to a more understandable format and includes links to community-backed sites that provide additional details which suggest the course of action to rectify the associated issue.
- Automatically generates alerts on key events, ensuring that critical events are identified in a timely-fashion.
- Complies with PCI DSS without wasting precious internal IT department resources.

GFI EventsManager is the automation solution that enables businesses to address all these challenges.

### GFI EventsManager

GFI EventsManager is a best-of-breed event log management solution that numbs the pain of manually managing Windows events, Syslogs and W3C event logs. It augments PCI DSS compliancy efforts by addressing the requirements of this directive through a wide array of features including remote event log collection and consolidation (across local network and networks that are geographically distributed), advanced event filtering, extensive event browsing and forensic investigation options, alerting on key events, as well as comprehensive reporting that provides tangible proof of compliance efforts.

A version of GFI EventsManager specifically customized for PCI DSS has been included in the specialized GFI PCI Suite. This suite also includes GFI LANguard N.S.S., a network vulnerability management solution, together with a package of tailor-made reports. For more information about GFI EventsManager and the GFI PCI Suite, and how these products assist your business to achieve PCI DSS compliance visit: <http://www.gfi.com/pci/>.

### Conclusion

PCI DSS compliance has now become the irrefutable responsibility of all businesses handling cardholder data including retail, mail orders, telephone orders and e-commerce - irrespective of size. To ensure network security



## Automated event log management for PCI DSS compliance

and meet the PCI DSS compliance deadlines, companies must give up on manual event log management and implement automated solutions that overcome the challenges posed by this daunting task. The underlying rationale behind such a requirement is the need for organizations to protect themselves... to be ahead of threat rather than passively reacting to it after that the damage is done.

### About GFI

GFI is a leading software developer that provides a single source for network administrators to address their network security, content security and messaging needs. With award-winning technology, an aggressive pricing strategy and a strong focus on small-to-medium sized businesses, GFI is able to satisfy the need for business continuity and productivity encountered by organizations on a global scale. Founded in 1992, GFI has offices in Malta, London, Raleigh, Hong Kong, and Adelaide which support more than 200,000 installations worldwide. GFI is a channel-focused company with over 10,000 partners throughout the world. GFI is also a Microsoft Gold Certified Partner. More information about GFI can be found at <http://www.gfi.com>.



### Sign up to GFI's FREE SMB-Zone Newsletter

Receive FREE invites to SMB focused content such as IT Advice,  
Topical White Papers, MVP Tips and Tricks, Webcasts and much more!

© 2009 GFI Software. All rights reserved. The information contained in this document represents the current view of GFI on the issues discussed as of the date of publication. Because GFI must respond to changing market conditions, it should not be interpreted to be a commitment on the part of GFI, and GFI cannot guarantee the accuracy of any information presented after the date of publication. This White Paper is for informational purposes only. GFI MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS DOCUMENT. GFI, GFI EndPointSecurity, GFI EventsManager, GFI FAXmaker, GFI MailEssentials, GFI MailSecurity, GFI MailArchiver, GFI LANguard, GFI Network Server Monitor, GFI WebMonitor and their product logos are either registered trademarks or trademarks of GFI Software Ltd. in the United States and/or other countries. All product or company names mentioned herein may be the trademarks of their respective owners