

## Straight Talking – As crunch bites, don't forget the logs

By Fran Howarth, Principal Analyst, Quocirca Ltd

Managing log files may seem like a mundane issue but doing it well tightens data security and boosts compliance efforts.

Managing risk, compliance and security are objectives that still need to be achieved even while organisations rush to cut costs.

The insider threat in particular has always been a key challenge for organisations and, with staff being made redundant in droves these days, access rights to sensitive company information must be revoked quickly.

The external threat is getting worse as well, as hackers are increasingly targeting corporate networks for financial gain. In January 2009 security technology vendor McAfee estimated that data theft and breaches cost businesses worldwide approximately \$1tr in lost intellectual property and expenditures for cleaning up the damage caused.

All organisations should take note. In an economic downturn, businesses switch focus from acquiring customers to retaining them. Any security breach where data is lost could damage their reputation and cause customers to jump ship.

Failure to adequately protect information and ensure its integrity has not been compromised could also lead to organisations being unable to comply with a growing roster of regulations requiring higher data security standards including: the Payment Card Industry Data Security Standard (PCI DSS); e-discovery requests, which are commonplace in the US and becoming more so in Europe; and security breach disclosure legislation, which is expected to be enacted in the near future by the EU.

Because of these factors, protecting data is now one of the top business-driven issues for improving security and managing risk.

In order to prove that security controls are effective and to be able to comply with potential litigation requests, organisations need to put in place an effective system for policing information governance, including the ability to organise, retrieve and analyse information, as well as to report on the effectiveness of controls over information access for audit purposes and for responding to litigation requests such as e-discovery.

This means establishing a system of electronics records management across the organisation, covering all data stores and including both structured data, such as databases, and unstructured information, such as emails and documents. The system must cover the entire lifecycle of electronics records - including when they are generated, backed up and archived - and must ensure the integrity of all records is maintained.

That in itself is a daunting enough challenge. But then there are the computer-generated log files. Log files provide granular information about activities by the hardware and software on your network, such as which machine tried to gain access to a particular server, at what time and on which date. Analysis of these log files allows an administrator to compare activities against expected norms and policies.

Log files may contain critical information that can throw to light anomalies, whether they are misconfigurations, inappropriate actions by individuals or evidence of other system vulnerabilities. They are the basis for proving the chain of information custody for governance purposes, in answering litigation requests, and in performing forensics to find out why something happened.

Collecting, storing and recovering log data is a hard task. They are largely undecipherable to humans, containing line after line of repetitive computer-generated code. According to the 2008 version of its annual log management survey,

the Sans Institute found just 35 per cent of respondents were satisfied with their log analysis capabilities. The most problematic issues cited by respondents were collecting log records, searching for and reporting on log data.

Among the problems are that logs are generated in a variety of inconsistent formats and must be enriched before they can usefully be indexed and searched.

Although log files provide important information about the security posture of electronic networks, log file management and analysis is a problem largely overlooked in many organisations.

Some do it manually - a tall order - while others use homegrown systems. Automated log management and analysis is a better way for organisations to discover and respond to security vulnerabilities that could compromise sensitive data.

By including log files in information governance plans, organisations can take control of data in all forms to minimise risk across the organisation. Some regulations place a lot of emphasis on logs. For example, the PCI DSS regulation requires that adequate controls are in place for log management, including collection, review, retention and destruction of those logs.

With compliance, cost control and security key objectives this year, organisations should look closely at the effectiveness of their log management. It may seem like a mundane issue but log files can help flush out vulnerabilities, shield organisations from risk and help them meet broader compliance objectives.

## About Quocirca

Quocirca is a primary research and analysis company specialising in the business impact of information technology and communications (ITC). With world-wide, native language reach, Quocirca provides in-depth insights into the views of buyers and influencers in large, mid-sized and small organisations. Its analyst team is made up of real-world practitioners with first hand experience of ITC delivery who continuously research and track the industry and its real usage in the markets.

Through researching perceptions, Quocirca uncovers the real hurdles to technology adoption – the personal and political aspects of an organisation's environment and the pressures of the need for demonstrable business value in any implementation. This capability to uncover and report back on the end-user perceptions in the market enables Quocirca to advise on the realities of technology adoption, not the promises.

Quocirca research is always pragmatic, business orientated and conducted in the context of the bigger picture. ITC has the ability to transform businesses and the processes that drive them, but often fails to do so. Quocirca's mission is to help organisations improve their success rate in process enablement through better levels of understanding and the adoption of the correct technologies at the correct time.

Quocirca has a pro-active primary research programme, regularly surveying users, purchasers and resellers of ITC products and services on emerging, evolving and maturing technologies. Over time, Quocirca has built a picture of long term investment trends, providing invaluable information for the whole of the ITC community.

Quocirca works with global and local providers of ITC products and services to help them deliver on the promise that ITC holds for business. Quocirca's clients include Oracle, Microsoft, IBM, O2, T-Mobile, HP, Xerox, EMC, Symantec and Cisco, along with other large and medium sized vendors, service providers and more specialist firms.

Details of Quocirca's work and the services it offers can be found at  
<http://www.quocirca.com>