

Information security: changing perceptions and changing realities

**Phil Neray, vice president
of security strategy at
Guardium, an IBM company**



Finger On The Pulse

The number of people who have experienced identity fraud due to data breaches pales in comparison to the number of people who fear it. But data breaches are a looming threat—they're not only costly to organisations in terms of fines, legal fees and increased audit costs, but also affect consumer perceptions and reputational risk. Data breaches can hit retailers, banks and government organisations, and they can be executed by external forces such as cybercriminals or internally by rogue employees and outsourced personnel.

In a recent IBM/Guardium survey, more than 800 respondents in France, Germany, the United Kingdom and the United States shared their views on the safety of their Personally Identifiable Information (PII) and credit card data. Despite a few variations from country to country, the sentiment of the respondents was largely the same: consumers are quite concerned about the security of their personal and financial data, and they perceive that governments, banks and retailers remain ill-equipped to protect it.

In fact, in a telling commentary on 21st-century perceptions, US consumers believe that they are more likely to have their identity stolen than to have their cars stolen! Of all the consumers surveyed, 80 per cent said they were either concerned or 'very concerned' about the security of their credit card information. The respondents had learnt from experience: 16 per cent of them have actually been victims of fraud before, while in the US those who had been hit by fraud had been hit hard. For more than 55 per cent of US victims, over one thousand dollars were involved and for an unfortunate three per cent, over ten thousand dollars.

In Germany, retailers were overwhelmingly seen as the least trusted in protecting consumers' data, as outlined by 64 per cent of respondents. Retailers were also highlighted as the least trusted by French respondents (34%) and those in America (38%).

In Britain, the majority said they had the least trust in their own government, with only 2 per cent stating they had complete confidence in British government organisations to keep their data safe. Despite banks being cited overall as the 'most trusted' organisations by the British, IBM/Guardium found that more than two thirds (72%) of UK respondents were concerned over their bank's ability to safeguard financial data from internal threats and disgruntled employees.

The playing field for information security is expanding as a growing variety of transactional channels are opened for an increasingly rich range of data formats: consumers swipe credit cards at shops, buy gifts from online retailers, perform their banking online, carry health insurance cards and submit their personal information to governments in multiple forms such as income tax returns and passport applications. From country to country, database security managers have to mitigate different causes for concern. In the US, 88 per cent of respondents professed concern for the security of their personally identifying Social Security Numbers, while in France 70 per cent worried about the security of their Carte Vitale health insurance cards.

In other countries though, this lack of trust is reserved for the retail environment. A surprising 60 per cent of Germans expressed concerns over their retailers' ability to protect their information, outpacing government organisations and finance as the least trusted sector in the country. Banks though were also unable to escape respondents' scorn with 73 per cent of Germans expressing some concern about the security of their financial information by financial organisations. This widespread anxiety should set off signal flares for those responsible for database security. Either data breaches, fraud and other information security issues are prevalent enough to strike apprehension into the hearts of the populace, or the public perceives a much greater security threat than actually

exists. In either case, business managers must rectify the situation.

We're also currently witnessing a boom in the public's technological literacy. With each RockYou, TJ Maxx or Hannaford breach, consumers are gaining new information about the potential dangers to their data. We found that both Germans and Brits are split 50/50 as to whether they are more concerned about internal or external data breaches of their personally identifiable information. Part of the public's concern about its sensitive information can be attributed to its developing knowledge on the subject. Industry must respond by transparently assuring clients about the depth of their data security precautions. To close the gap between perception and reality, organisations need to keep the media alert, informing the public about how and why breaches occur, and what they're doing to prevent them in the future. Restoring public confidence is challenging but not unrealistic.

To truly win back confidence, organisations must do more than bring good news; they must educate their employees about data security, and they must maintain a secure data infrastructure. Too often, management is lulled into a false sense of security because they've deployed traditional perimeter defences such as firewalls, and they're passing their audits. However it's clear that this is no longer sufficient. In 2009, Heartland was the victim of the largest data breach in history, due to a SQL injection attack by cybercriminals operating in the U.S, Latvia, the Ukraine and the Netherlands, that ultimately resulted in the theft of 130 million credit cards—yet Heartland had standard firewalls and anti-virus systems installed and had recently passed their Payment Card Industry-Data Security Standard (PCI-DSS) audit.

In order to protect themselves, organisations need to implement continuous, real-time monitoring of all access to sensitive data, including

Finger On The Pulse

access by “superuser” employees and outsourced personnel on the inside. Most organisations still rely on manual review of logs to identify unauthorized activities, but this is time-consuming and inefficient, and also ineffective due to the massive amounts of transactions that occur at the database layer, so that spotting suspicious activities becomes equivalent to trying to find the proverbial “needle in the haystack.”

At one point in time, auditing all transactions also took a significant toll on system performance, but now data security technologies have moved forward. New database activity monitoring (DAM) appliances analyse all activity without any reduction in performance and without requiring changes to applications or databases. Any suspicious or

malicious behaviour can be immediately spotted by comparisons to normal activity baselines and corporate security policies. If any security problems develop, administrators can stop them before they start or proceed too far.

The development of reliable, responsive database activity monitoring has moved information security in the right direction, but it must be part of a continuing improvement effort. The best way to change public perception of data security is by changing the reality. In order to convince customers that their information is safe, their information must, in fact, be safe. Hackers and disgruntled employees will always redouble their efforts to crack security systems, so database security and monitoring must be doubly proactive, staying ahead of all threats.

Thorough data protection demands investment, but these costs pale in comparison to those associated with a data breach. Legal fees, fines, informing consumers, the cost of mandated annual audits, reactively securing data, restoring trust—these each have serious implications. Organisations would be wise to make a sound initial investment to safeguard data rather than waiting to respond to a devastating problem. It’s easier to pay to stay out of the news than to extract your brand from bad news. Besides, customers only notice security when something goes wrong

For a full copy of the IBM/Guardium findings please email prompt@prompt-communications.com