

**Experts in database security warn IT managers of impending security threats to data and urge them to get to grips with their database now or face the consequences in 2007**

***Know your database, its capabilities and its users, as new and emerging threats to IT will come in all shapes and sizes, even human***

18 December, Oxford – Secerno, the innovator in database and application assurance for the protection of online digital assets, urges IT managers to shift their focus inwards, take control of their databases and be prepared for the next wave of external and internal threats facing them in 2007.

Secerno's Chief Executive, Paul Davie, says 'It is fair to say that the security sector has now come to terms with the fact that they are dealing with highly financially motivated, technologically advanced and professional database infiltrators. The years of spam and simple phishing scams targeted at the naïve PC user are no longer our major concern. Any company that stores data needs to shift its focus inwards.

'In 2006, we witnessed overwhelming attacks on the storage and security of confidential financial data. Emails lured online bankers to provide their logins, passwords and account details, only to become victims of fraudulent activity or a complete loss of funds. Employees were blackmailed or bribed to download data for criminal gangs. Banks' websites were duplicated to provide a false sense of security and even the NHS' data was delved into, as Tony Blair's medical records hit the headlines.

Paul continues, 'So, what can we expect in 2007? Well, online banking is expected to increase as more than 16 million of us continue to login to our private financial data via websites. More than 26.4 million people now shop online with an estimated 372 million transactions being undertaken last year<sup>1</sup>. This number will increase in 2007 as we continue to shop from the comfort of our office or home. All of which will continue to attract the criminal organisations. Thankfully, a combination of recent high profile breaches and forthcoming legislative requirements, such as the PCI framework, is driving attention to the implementation of effective data security. Analyst predictions will be born out as database assurance proves to be one of security's hottest sectors in 2007.

More worryingly, we are due to see the UK's Integrated Children's System go live – a data system containing details of all of the nation's vulnerable children. This is madness of course – an incredible resource for child abusers the length of the country. Two questions spring to mind: will the first big story be of an external hack into the system or an authorised user abusing their access rights to find their targets? And, who will be hung out to dry: the poor soul responsible for specifying the system's security, or the politician who thought this was a good idea in the first place?

---

<sup>1</sup> Statistics supplied by APACS, the UK payments association



Returning to the finance world, Davie continues, “SQL Injection attacks – examples of which include hackers exposing hundreds of thousands of credit card numbers worldwide – certainly will increase sharply. In fact, SQL injection attacks have been increasing at a rate of more than 250% per year for the last few years. In 2007, SQL injection will be recognized as the number one attack vector on internet-facing systems.

‘We have to remember that humans make mistakes too, whether by accident or for financial gain. Enhanced internal attacks will continue to thrive as organised criminal gangs plant employees inside businesses. Recent statistics from the Secret Service and CERT show that 86% of computer sabotage is done by savvy IT staff within the organisation. Expert penetration testers see success rates of targeted attacks on databases approach 100%, when initiated from inside the organisation.

‘On the other hand, and without added conspiracy, we hear of laptops being misplaced, lost or stolen, leading to the possible loss of valuable data. But in 2007, for the first time, the number of published security breaches to confidentiality through database attack is expected to exceed those from lost back-ups and laptops.

Davie says, ‘At Secerno, we know databases and how they behave when attacked. We regularly see the database administrator (DBA) working with ‘blindsight’ - a DBA inherits a database and takes responsibility for managing and upgrading it, without concise and clear knowledge of its abilities, its strengths and its weaknesses. This approach to database management will be very costly in the long run, as it will affect the performance, scalability, future capabilities, usability and, naturally, the security of the critical business data. We urge IT directors to detect and prevent application intrusion, by removing the ‘blindsight’ approach, by understanding and becoming familiar with the behaviour of the database and its usage. The good news for 2007 is that the technology is there now automatically to measure database behaviour, allowing control and, at last, protection.

### **About Secerno**

Secerno products deliver the most sophisticated and effective solution for data and application security on the market. Secerno protects against internal or external, known or unknown database threats, and assures the integrity and privacy of your data. Secerno’s award-winning machine learning technology forms a concise, manageable and clear description of application and data behavior in real time. This enables accurate monitoring, trapping, reporting and auditing of *any* and *all* abnormal or inappropriate attempts to access key business data. Secerno introduces an unprecedented level of control, protects your reputation and assures the safe use of data, to support business growth. See [www.secerno.com](http://www.secerno.com).

### **For more information:**

Jane Folwell  
Folwell PR  
Tel: 01344 845132  
Mob tel: 07950 033370  
Email: [jane@folwellpr.co.uk](mailto:jane@folwellpr.co.uk)