

New Survey Reveals 77 Per Cent of Security Professionals Back UK Data-Breach Disclosure Law

6 July 2007 – The push for the European Directive on Data Protection to be passed as UK law is gathering pace, according to database security company, Secerno. A survey of IT security professionals at Infosec 2007 found that 77 per cent believe companies should be obligated by law to disclose when they have been the victim of a data security breach. The survey also found that of those in favour of such a law, nearly half (49 per cent) believe that companies should be forced to disclose a data breach immediately rather than delaying the announcement.

Even greater concerns regarding data security have also been voiced outside of the IT community. Independent research recently conducted by Ipsos MORI found consumers to be even more concerned about data breaches – 82 per cent expect to be notified immediately if there has been a security breach and their personal details have been compromised. Upon hearing of a data breach, most consumers (53 per cent) would vote with their feet and stop using the affected organisation's services immediately.

Paul Davie, founder of database security company, Secerno, comments: "Unfortunately, we don't know the scale of all data security breaches in the UK. Statements from the US-based Privacy Rights Clearing House suggest 100m records have been exposed during their two years of monitoring such events. In the UK, there is no legislation which demands the publication of such breaches, so the extent of the problem here is hidden – any of us could have been affected; we often don't find out until it's too late.

"There is a clear demand from security professionals and consumers that the Government and the EU should follow the US's lead and impose a legal framework that forces companies to disclose breaches. A situation that mirrors the infamous TJX breach may already have happened in Europe, but companies operating in this region are not legally obliged to notify their customers – which only erodes public confidence."

Davie believes that far-sighted companies are beginning to realise that pre-empting an EU directive on data breaches is good for public confidence – and for business: "High-profile breaches have evidently rocked consumers' faith in the ability of large organisations' to protect their personal data. Consumers are demanding that they be informed immediately whenever a breach occurs, and in the event of a breach they are unafraid of taking the most damaging action – withdrawing their custom immediately.

"Rather than passively awaiting the appropriate legislation from the EU, there is an opportunity for organisations to take it upon themselves to reverse the swell of negative public opinion by implementing database security technology. In doing so, they can prove to the public that guaranteeing the protection of their personal details is of paramount importance to them, which will help rebuild consumer confidence and, ultimately, drive business growth."

A change in mindset may be required, however, before companies grab this opportunity. Says Davie: "Many businesses make the mistake of believing data security to be just an IT issue, when it's evidently more important than that – it's a business issue that needs managing from the board level."

Florida's Attorney General McCollum recognises the importance of protecting consumers from the threat of identity theft. "Identity theft steals not only money, but also a person's good name and reputation. Any effort made by corporate entities to protect customers from identity theft is a positive step in the right direction."

About Secerno

Award-winning Secerno provides the world's most advanced, comprehensive and intelligent database security solution.

Deploying a microperimeter approach, Secerno.SQL sits right next to an organisation's data asset to protect data at the highest level. Its unique machine-learning technology understands the true intent of database interactions and protects an organisation's data from both known and unknown threats to data, whether they originate from external or internal sources.

Located in Oxford, UK, Secerno enables the continuous improvement of data security by allowing companies to understand, control and protect their data assets. It empowers organisations to derive the most value from their information and to enable data security without the costs associated with traditional solutions.

Secerno offers protection to customers across an array of industries including financial services, healthcare and pharmaceuticals, retail and government agencies and departments. Secerno is funded by UK investors, including Eden Ventures, Quester and Oxford Venture Management, who have a successful track record for backing winning innovators and entrepreneurs.