Avoiding online security breaches

By Alan Pedersen

AS MORE ORGANISATIONS start to move their customer databases online, the risks of accidentally exposing personal information grow. *PL&B International* looks at the legal risks and how organisations can avoid falling into the trap.

High profile cases of organisations accidentally exposing customer details online are somewhat rare these days. Nonetheless, large organisations are still being caught out. One of the most recent cases involved retail giant, Tower Records. Back in December the music retailer confirmed a report by *News.com* which claimed that over three million UK and US customer accounts were left unprotected. Although no credit card details were revealed, a programming error on the company's website meant that anyone hooked up to the Internet was able to access postal and e-mail addresses, telephone numbers and purchase histories.

Paul Hopkins, security health check manager at UK consultancy firm, QinetiQ, says these incidents were more common in the early days of e-commerce and now appear to be tailing off. "I think a lot of the accidents were caused by inexperience as well as the rush to market. A lot of the big companies now have some good security policies in place, mainly through development and education of their programmers."

Identifying flaws when designing websites is not straightforward, says Hopkins. "It's very easy to check the functional requirements, but difficult to test the unknown dangers. Companies need to look at training their staff to understand the security issues of their programming and then also look at comprehensive testing throughout – as they develop the system and not just at the end."

One such example is when Microsoft took 11,000 programmers away from their jobs in February 2002 to train them in writing secure code.

AVOIDING LEGAL ACTION – US AND UK PERSPECTIVES

The Tower Records incident could well have prompted legal action from UK and US regulators. So, how would they view such a breach, and what is the likelihood of enforcement action?

Nicholas Graham, solicitor at Denton Wilde Sapte, says that there are no specific recommendations under the UK Data Protection Act for web security, simply because laws cannot keep pace with technology. Instead, organisations are advised to adopt the broader concept of "best practice".

"By adopting and maintaining best industry practice you stand the smallest possible chance of a breach of principle seven," says Graham. [Principle seven of the Data Protection Act relates to security of personal data.]

He recommends that organisations consider implementing the ISO 17799 security standard, adding that although several thousand companies have implemented the standard, it is "still of relatively limited impact."

Despite the complexity of security breaches, Graham says that it would still be relatively straightforward for the Office of the Information Commissioner to prove a security breach. "The way in which they would measure a breach is by reference to the successful prevention of unauthorised damage to, or disclosure of personal data." So, an organisation under investigation may find its security practices being benchmarked against similar companies.

Legal action is especially problematic for US organisations, says Kirk Nahra, an attorney for Washington-based Wiley Rein & Fielding. "One of the difficulties that US companies face is that they can be attacked from a variety of directions." These include state attorneys general, the Federal Trade Commission and specific sector-related regulators. However, says Nahra, "the biggest wildcard, depending upon what happens in the security breach, are lawsuits, because they can come at the slightest provocation."

When it comes to regulatory action, Nahra says organisations are more concerned about the changes imposed on their business practices than actual financial penalties. While fines are relatively low, an organisation may be forced to implement stricter standards that current laws require.

ASSESSING THE LEGAL RISKS

The risks for UK companies, says Graham, will depend upon "the extent to which the Commissioner is really prepared to take action as opposed to just giving them a slap on the wrist. Because I think that is what has happened in some cases in the past."

According to Nahra, US regulators lack the financial muscle to aggressively tackle non-compliance issues. For example, he says that the government agency responsible for enforcing the HIPPA (healthcare) privacy and security laws has publicly stated that it does not have the money, budget, or staff to adequately enforce the law. If there is little risk of regulatory action, then some companies may see little point in struggling to implement the strictest security standards.