Online business plays catch-up on privacy

By Alan Pedersen

AS E-COMMERCE SPEEDS ALONG the broadband superhighway, corporate privacy practices are stuck in the slow lane, struggling to keep up with the pace.

Speed to market has often been the corporate mantra of many online business strategies. But while the tech-heads and marketers have forged ahead, creating ever more complex and sophisticated websites, compliance officers have been left to cope with a bewildering array of privacy problems.

More than just a weak theory espoused by paranoid web users, there is now a wealth of respectable research to suggest that privacy has become one of the key challenges in the online world. Finally, however, businesses seem to have caught on to the fact. According to a recent survey by website management solutions provider, Watchfire, 87 per cent of the companies they questioned regard privacy issues as "somewhat" to "very important".

EASIER SAID THAN DONE

Recognising the importance of privacy is one thing. Providing an adequate and efficient system for managing it, however, is an altogether different matter. Less than half of the organisations surveyed by Watchfire have formally stated privacy policies on their website. What makes this interesting is that they are not small businesses. 20 per cent of the 600 mainly North American-based organisations that were surveyed have annual revenues in excess of $1 billion.

Even those organisations that do post privacy policies on their websites may be lulling themselves into a false sense of security. "We often find that there's a difference between what the policy says and what people actually do," says Michael Weider, Watchfire's chairman and chief technology officer. Privacy policies do not necessarily guarantee privacy – even the most basic things can be overlooked. "I've yet to see a website that doesn't have some issues on it," says Weider.

LACK OF COMMUNICATION

Often this is due to the fractured nature of large organisations. Because many organisations have different business units with different go-to-market strategies, websites are often developed in isolation, says Brendon Lynch, a privacy and data protection specialist at PricewaterhouseCoopers. "There may be a gap between those at the corporate level who are trying to institute good policy and manage risk, versus those at a business unit level who are really just trying to further their business," he says. According to Michael Weider, this invariably leads to a disconnection developing between the two, "because the left hand doesn't know what the right hand is doing."

This can cause real problems and leave businesses open to a number of potential privacy breaches. Marketing departments using the latest profiling and tracking technologies could be collecting information on customers without their knowledge or consent. You only have to look at the recent US settlement cases with Microsoft and DoubleClick to realise how important this area is becoming (see p.3 and p.15).

Organisations may need to pay more attention to the use of cookies on their websites. Microsoft's latest web browser, through its incorporation of P3P-enabled cookie blocking technology, could affect the functioning of some websites. Yet 28 per cent of the organisations surveyed by Watchfire are completely unaware of the P3P protocol and the impact it could have on their business.

Poor security design on website registration pages can also raise privacy problems, with data spillage potentially leaving customer information exposed or passed onto unauthorised third parties. Only last month an online shopping site in the UK inadvertently exposed the details of nearly 2,000 customers on its website.

Even those companies with compliance teams or privacy departments are struggling to keep track of their organisation's privacy practices, and it is not going to get any easier. "The earlier sites were relatively primitive and small," says Weider, "so it wasn't as difficult to keep track of everything." But nowadays, with the amount of online content increasing at a phenomenal rate, some corporate websites can often sprawl across hundreds of thousands of web pages. There is also much greater online interaction between consumers and businesses, creating a greater potential for privacy breaches to occur.

MONITORING COMPLIANCE

So, how do businesses fare when it comes to managing such a difficult task? According to Watchfire, only 40 per cent of the businesses it surveyed actively monitor their websites for privacy compliance. Of those that do, 83 per

cent said they used manual monitoring methods. This, suggests Weider, is an enormous drain on resources. In addition to the huge amount of time that would be spent trawling through thousands of web pages, human error means serious privacy breaches could be missed. Technology solutions that can continuously analyse website compliance, argues Wieder, act as a "far more sophisticated approach" to the problem.

The need for automated compliance solutions is not just restricted to privacy issues. The management of hyperlinks to third party websites is a prominent issue. Third party websites can fall prey to "porn-nappers" and other dubious businesses which take over domain names when website registrations expire. This can indirectly impact the reputation of websites that publish these links. Of the 600 organisations surveyed by Watchfire, 77 per cent monitor third party hyperlinks, yet only 9 per cent use automated solutions. According to Pricewaterhouse Coopers, the fact that some websites can have in excess of 10,000 external links means that effective manual monitoring becomes impossible.

As organisations expand the online side of their business, there is an ever-increasing need to address privacy. Organisations need to create an "understanding of what it really means to make a website fully privacy friendly," says Brendon Lynch. He argues that because there are hundreds, if not thousands, of people contributing to the development of a company website, education and awareness is key to achieving a privacy compliant website.

Monitoring for website compliance through automated solutions will also "become an integral part of the compliance programme," says Lynch. The take-up of these compliance solutions, he says, will increase as the technology matures and becomes tailored to suit the individual needs of each company.

The findings from Watchfire's survey, along with additional commentary provided by PricewaterhouseCoopers, is available from: www.watchfire.com/resources/risk-rpt-july02.pdf

Network cyber attacks on the increase

By Eugene Oscapella

US-based security firm, Riptech, claims that Internet attacks on computer networks grew at an annualised rate of 64 per cent between January and June 2002.

Riptech's findings, part of a report released on July 8th, were derived from a sample set of more than 400 companies in over 30 countries.

Among the specific findings:

• Internet attacks have increased at a 64 per cent annualised rate in the six-month period.

• 80 per cent of all attacks originated from only 10 countries, up from 70 per cent during the previous six-month period – United States, Germany, South Korea, China, France, Canada, Italy, Taiwan, Great Britain, and Japan.

• 70 per cent of power and energy companies suffered a severe attack, compared to 57 per cent in the previous six-month period

• Public companies were twice as likely to experience at least one severe attack and were also twice as likely to suffer a highly aggressive attack than private, nonprofit, and government entities combined.

Testifying before a US House of Representatives committee on July 24th, Riptech founder Tim Belcher observed that allowing easier access to operational, customer, and supplier information, combined with the expansion of corporate information technology boundaries, vastly increased network vulnerabilities. Among the more common vulnerabilities he identified were: excessive employee access, excessive "trust" of third parties (for example, contractors and consultants), poor network configuration, inadequate password protection, unintended "dial-up" and/or wireless access, and improper network segmentation (setting up separate networks to operate critical infrastructures).

Belcher noted that power, energy, and financial services companies experienced the highest rate of overall attack activity. They also suffered relatively higher rates of severe and highly aggressive attacks during the preceding six months. "I think it is clear that critical infrastructure companies are experiencing a high rate of attacks from sources that may be targeting them for a particular reason... It is clear to me that critical infrastructure companies need to be more diligent in protecting their networks." Later, he observed that "we have relied too much on luck in the past to protect us from a truly catastrophic incident involving cyber-intrusions, [but] critical infrastructure companies have the ability to create adequate protections from a majority of the dangers they presently face."

Further information:

www.riptech.com/newsevents/release020708.html; www.riptech.com/newsevents/release020724.html; http://reform.house.gov/gefmir/hearings/2002hearings/0724_cyberterrorism/belcher_testimony.htm.