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.