



CYBERBLUDGERS BEWARE

Management Needs to Curb the Costs and Risks of Non-Work-Related Internet Activities, Writes Darren Horrigan

Few people know that, fresh from bashing Rodney King near to death on a Los Angeles street in 1992, LAPD officer Lawrence Powell sent this e-mail to a work-mate: "Oops! I haven't beaten anyone that bad in a long time." At his trial, prosecutors let Powell explain his actions on the infamous videotape of the incident as "necessary force" before presenting his smart-mouthed e-mail as further evidence he was a racist cop. Powell went to prison. King became a millionaire.

In her autobiography, Monica Lewinsky speaks of the "violation" she felt during the Starr investigation when deleted e-mails, some two years old, were retrieved from her office computer. In many, she refers to the man with whom she shared cigars as "The Big Creep". One e-mail read: "I want to hug him so bad right now I could cry." Everyone did, later on.

This is the real power and treacherous nature of workplace e-mail – a fact also well appreciated by what's left of Enron, Andersen, One.Tel and HIH.

Company lies, staff secrets, dirty jokes, smutty pictures and gossip about the boss have always been part of the workplace. Companies tolerated such behaviour as long as it didn't offend anyone or get in the way of real work.

But technology has shattered that informal agreement. Sophisticated enterprise software that allows companies to share closer links with customers, partners, suppliers and distributors also creates security weaknesses. The proliferation of technology tools among employees is one of the reasons 2002 will be remembered as the year in which Australian companies came to respect the importance of internal security.

International Data Corporation (IDC) estimates 15 billion e-mails are sent throughout the world each day, a number that will double in the next three years. Do work responsibilities make us such voracious users of e-mail?

No, say most of the world's major web research firms and security software vendors. They call it "cyberbludging."

Gartner estimates that non-work-related surfing costs United States companies \$54 billion in productivity every year. According to the July 2000 "Cyberbludging Report" from the e-mail-filtering software company SurfControl, the annual figure in Australia is a relatively trifling \$300 million. Management knows it has to be vigilant because every joke, photo, cartoon and whinge sent by e-mail leaves a record, somewhere. A single complaint from one person who saw a single offensive sentence, picture or web site can ruin reputations, destroy careers and cost big money.

The world's most expensive e-mail, for example is "25 reasons why beer is better than women" – you can share a beer with your friends is just one "reason" CFO can print. This piece of supposedly harmless sexist drivel cost Chevron, the US resources company, \$US4 million in a 1995 harassment settlement.

But the costs and consequences of non-work Internet use hits a company in many ways other than legal liability: staff morale, productivity, bandwidth wastage and security, to name a few.

E-mail is now the most dangerous tool in the workplace because it gives disgruntled employees a new weapon with which to wreak havoc and, by providing an easy conduit in and out of a company, increases the likelihood of confidential information being lost or computer viruses infecting a network.

WebSpy, a Perth developer of Internet monitoring and management tools, tells the tale of the Australian CFO who was surfing pornography on the Internet when he downloaded a file that contained a virus. The virus, which escaped detection by the company's anti-virus software, trashed the CEO's hard drive and then propagated throughout the entire network of 30 computers and servers, destroying all of the company's data files. The firm lost a year's worth of data and weeks of productivity.

Says WebSpy CEO Jack Andrys: "While most employees don't abuse their e-mail or Internet privileges, those who do cost companies dearly, not only in lost productivity but also in potential security hazards and legal minefields."

The Fourth Amendment to the US Constitution provides privacy protection for Americans, but there is no such constitutional or common law right to privacy in Australia. It had been legal for Australian employers to monitor in secret an employee's use of e-mail and the Internet, but now provisions to the Privacy Act mean employees must now be told when and why they are being monitored.

According to the US-based Privacy Foundation, there are about 100 million people around the world who have Internet and/or e-mail access at work. More than 27 million of them are under continuous surveillance. An example of the intrusive nature of some surveillance products is Spector, software that can record every keystroke a user makes. It automatically takes screen snapshots each couple of seconds. This is the type of software that got 40 Xerox workers sacked in 1999 for surfing forbidden web sites. Today, Xerox routinely monitors the web use of every one of its 85,000 employees worldwide. New York-based Xerox spokesman, Bill McKee, says the surveillance is no secret.

Charles Heunermann, the managing director of SurfControl Australia, says management should work with employees to establish policies about appropriate web surfing.

Non-work-related Internet activities can also have a devastating effect on a company's bandwidth usage. Employees who download music, pay bills online, play games or just browse the web impede the work-related activity of colleagues. The bandwidth problem becomes acute during peak periods of personal e-mailing. Servers often crash on Valentine's Day and around Christmas. Online shopping leaps in the lead up to Mother's Day, Father's Day and Easter. Temptation proves too great for some during one-day cricket matches, the start of the footy season and during special events such as the World Cup Soccer.

But workplace Internet and e-mail shenanigans will continue, of course. As we muddle through the maze created by human frailty and the incompatibility of technology with the law, we'll be reminded of those words of Marshall Metuhan, circa 1964: "We shape our tools and, thereafter, our tools shape us."

CFO Magazine