

# Do YOU Put Your Workplace At Risk?

-- European Study Lists Insider Threat Statistics --

McAfee, one of the two best-known retailers of anti-virus software reports that:

- One in five workers (21%) let family and friends use company laptops and PCs to access the Internet.
- More than half (51%) connect their own devices or gadgets to their work PC.
- A quarter of these do so every day.
- Around 60% admit to storing personal content on their work PC.
- One in ten confessed to downloading content at work they shouldn't.
- Two thirds (62%) admitted they have a very limited knowledge of I/T Security.
- More than half (51%) had no idea how to update the anti-virus protection on their company PC.
- Five percent say they have accessed areas of their IT system they shouldn't have.

Based on its survey, McAfee has identified four types of employees who put their workplace at risk:

- **The Security Softie** – This group comprises the vast majority of employees. They have a very limited knowledge of security and put their business at risk through using their work computer at home or letting family members surf the Internet on their work PC.
- **The Gadget Geek** – Those that come to work armed with a variety of devices/gadgets, all of which get plugged into their PC.
- **The Squatter** – Those who use the company IT resources in ways they shouldn't (i.e. by storing content or playing games).
- **The Saboteur** – A very small minority of employees. This group will maliciously hack into areas of the IT system to which they shouldn't have access or infect the network purposely from within.

**INTERNAL THREATS** Second only to hackers, 29% of cyber security threat come from insiders – employees and contractors. Other studies have estimated the internal risk as high as 50%. Unfortunately, while the inside threat is less frequent it is often more deadly. Insiders already have access to your systems and are often the only resource your company has for security. Some examples:

*A system administrator, angered by his diminished role in a thriving defense manufacturing firm whose computer network he alone had developed and managed, centralized the software that supported the company's manufacturing processes on a single server, and then intimidated a coworker into giving him the only backup tapes for that software. Following the system administrator's termination for inappropriate and abusive treatment of his coworkers, a logic bomb previously planted by the insider detonated, deleting the only remaining copy of the critical software from the company's server. The company estimated the cost of damage in excess of \$10 million, which led to the layoff of some 80 employees.*

**An application developer**, who lost his I/T sector job as a result of company downsizing, expressed his displeasure at being laid off just prior to the Christmas holidays by launching a systematic attack on his former employer's computer network. Three weeks following his termination, the insider used the username and password of one of his former coworkers to gain remote access to the network and modify several of the company's web pages, changing text and inserting pornographic images. He also sent each of the company's customers an email message advising that the website had been hacked. Each email message also contained that customer's usernames and passwords for the website. An investigation was initiated, but it failed to identify the insider as the perpetrator. A month and a half later, he again remotely accessed the network, executed a script to reset all network passwords and changed 4,000 pricing records to reflect bogus information. This former employee ultimately was identified as the perpetrator and prosecuted. He was sentenced to serve five months in prison and two years on supervised probation, and ordered to pay \$48,600 restitution to his former employer.

**A city government employee** who was passed over for promotion to finance director retaliated by deleting files from his and a coworker's computers the day before the new finance director took office. An investigation identified the disgruntled employee as the perpetrator of the incident. City government officials disagreed with the primary police detective on the case as to whether all of the deleted files were recovered. No criminal charges were filed, and, under an agreement with city officials, the employee was allowed to resign.

These incidents of sabotage were all committed by "insiders:" individuals who were, or previously had been, authorized to use the information systems they eventually employed to perpetrate harm. Insiders pose a substantial threat by virtue of their knowledge of, and access to, employer systems and/or databases.<sup>ii</sup>

How do most employees endanger their organization? They don't establish secure systems, and don't create a business framework that supports data security and privacy.

How can you assess your corporate risk? Get an assessment from an outside firm recommended by an external source – maybe your audit firm or a privacy security consultant. But there are some warning signs that even the technically-challenged can look for:

- Do you have an open technology strategy – data sharing for maximum information exchange?
- Does it offer an opportunity for people to match data? A huge database that contains copies of all sensitive documents. A search engine looks for exact matches in documents at rest or in motion within the network.
- Does it create an index that makes it possible to find pieces of information taken from the documents?
- Does management have a distributed security strategy so that there are checks and balances in place?

Information is power, and stolen information, particularly by an insider, is a huge risk. Act accordingly.

---

<sup>i</sup> Bruce Schneier on the Insider Threat: *December 19, 2005*

<sup>ii</sup> U.S Secret Service and CERT Coordination Center/SEI Insider Threat Study: Computer System Sabotage in Critical Infrastructure Sectors, May 2005