Strauss vs. microsoft corp

Business, Company

In 2003, the United States government created what it termed as the National Strategy to Secure Cyberspace. This strategy was composed of five components that are as follows in direct quote: a cyberspace security response system--a network through which private sector and government organizations can pool information about vulnerabilities, threats, and attacks in order to facilitate timely joint action; a cyberspace security threat and vulnerability reduction program, consisting of various initiatives to identify people and organizations that might attack U. S. information systems and to take appropriate action in response;

A cyberspace security awareness and training program, consisting of several initiatives to make the public more vigilant against cyberthreats and to train personnel skilled in taking preventive measures; an initiative to secure the governments' cyberspace, which includes programs that state and federal government agencies will take to protect their own information systems; and national security and international cyberspace security cooperation--initiatives to ensure that federal government agencies work effectively together and that the U. S. government works effectively with foreign governments.

This was a true wake up call to the IT (InformationTechnology) companies such as Microsoft. As each year advanced, the cost to keep this security risk mounted, estimating into the billions of dollars. Yet, the effectiveness of this situation had produced mostly unsatisfactory results, according to the FBI-sponsored survey taken by CSI (Computer Security Institute) in 2002. After the survey, it was noted that fewer of respondents to this survey actually could show proof that they had acquired enough financial offset to justify the cost of the programs.

The CSI survey was regarded as statistically favored in certain respondents. Its validity was questioned. After September 11, 2001, the demand for improved internet security tripled and even people who were not " internet savvy" became well aware of the threats to their livelihoods and their lives. It was a clarified statement that just four possible viruses could cause more estimated financial damage that a natural disaster or terrorist attack on a major city or government facility. Yet did Microsoft step up to the challenge?

One factor of internet security that is of major importance became the effect of e-mail, both in personal and business use. Since most large companies had moved into almost complete computer controlled business aspects, any type of office worker had access to at least one computer or more. Companies found that their employees were accessing non-work related web sites and also using the company e-mail addresses for personal use, therefore, reducing the employee's productivity while costing the company labor hours with no profitable use.

A call went up for monitoring systems to supervise such wanton activity as employee viewing of porno sites and also using their business computers to chat with friends andfamily. The business e-mail set became the fastest way to have inner office response such as memos or contact from supervisor to employee. Microsoft developed a program to log a record of all e-mail use so that the company management could have a printed record of what passed through their computers. It worked to their advantage and disadvantage as it was a double sided blade.

It allowed the supervisory staff to catch employees abusing their computer privileges which could lead to write ups and eventual dismissals but it also caught many upper staff management plus other employees in the act of sexual harassment of other employees. This also lead to cases of racialdiscriminationand personal harassment of certain employees and could be used as a means to prove these cases when the employee felt they were denied promotion on the aspects of race, gender, age or sexual preference. Such activities led to a lawsuit being filed against Microsoft for just these various reasons.

In the 1995 case of Strauss vs. Microsoft Corp. (U. S. District Court for the Southern District of New York), a female employee of a Microsoft publication claimed that her supervisor made offensive messages and sexually explicit e-mails to her. Microsoft stated that the messages were intended to be funny and not meant to be offensive. Microsoft lost and the court's decision had a resounding effect on similar cases that were filed afterwards. Companies discovered that monitoring an employee's internet activities could be costly if there was any type of unbecoming behavior linked to the system.

It increased the government policy of sexual harassment awareness and companies were required to adopt almost a zero tolerant policy on the subject but the upside was that employees became more productive and spent less time in using their business computers for personal use. It did cut down on the possibility of any e-mail virus slipping past the company's system undetected. The monitoring severely decreased the chances of sharing business material to other possible rival companies.

The Strauss lawsuit was a direct hit to Microsoft to continue to upgrade the security in their products in business. Little known is the fact that e-mail accounts can be monitored, whether business or private, such as by the government or other interested parties with the clearance to do so. So how safe is e-mail? Not nearly as most people tend to believe. Under certain circumstances, employees’ personal e-mails can be protected under the NLRA (National Labor Relations Act) when the e-mail is used to address issues in dealing with company policy and the employee’s disgruntlement of that policy.

If an objector tone is used in the e-mail to a supervisor which is an expression is displeasure over a policy, the employee can be protected under the NLRA from dismissal or any other disciplinary action. The securities for businesses that use the monitoring system are protected in many ways but also unprotected in many others. Microsoft’s development of this system has had mixed reactions but still the pros have to outweigh the cons in the overall picture.