

The Importance of Cyber Security

The Internet is an indispensable communication tool

The Internet has changed the lives of many people. Some use it purely as a research tool, but for most people it has become an indispensable communication tool and as an integral part of their daily lives. The power of the Internet reverberates around us. As the Internet goes mobile and becomes ubiquitous, it is becoming significantly hard to go about our daily lives without access to the Internet.

Businesses, large corporations and small companies alike, have also integrated the Internet in their daily operations. As businesses' operations have become more complex, online applications for commercial use have evolved to become more sophisticated, and to better able to accommodate the demands of organizations such as data storage, [virtualization](#) (like [VMware](#)), cloud computing, IP-based communication, data transfers and email.

These days, it is fairly safe to say that the Internet has become an indispensable tool for business processes as well. For most businesses, the Internet has served not only as a tool, but as a platform upon which their business processes are built and performed.

But as more and more vital business information are being stored, exchanged and transferred within the "Information Superhighway", data security has become a major concern. [Cyberterrorism](#), a virtual crime aimed at not only pirating vital information



exchanged on the Internet, but as well as attacking and compromising key data-storage points and IT infrastructure, is a real threat that should not be taken for granted.

Cyber-terrorism – A continuing threat to corporate information security

Companies with huge amounts of key information stored in their computers are a delectable target for cyber-terrorists. The most dangerously sophisticated among the cyber-terrorists has the capacity to disable an entire economic system. That is why small businesses with very limited IT security set in place should take the necessary steps in beefing up their information security before any attack can even partially disable their business. With each passing time, neglecting to impose the necessary IT security measures potentially exposes your entire business to a host of malicious software that could take down your business anytime.

Points of entry

Just as conventional terrorism has points of entry, such as airports with poor security systems, bus terminals and seaports, cyber-terrorists also have their unscrupulous means of indentifying vulnerabilities in IT systems. Without proper security software in place, malicious software could penetrate your business' local network through email and social networks. Just recently, social networking giants Twitter and Facebook suffered quite a number of cyberspace attacks, causing damage to local computers on some of their members' ends.

How to practically protect your IT infrastructure



The full responsibility of setting up a strong business [IT security](#) system in place rests upon the company's management. Enforcing a strong corporate stand on the use of social networks in the workplace, for example, is a good step towards winning the battle against cyber-terrorism.

However, this is just part of the game strategy. Responsible leadership calls for the exploring of the services of reliable IT support firms. Calling on the service of qualified [IT consulting](#) companies minimizes the risks to your company's data, network and users by recommending strategies that are unique to your company's requirements.

Your company should also set strict policies that restrict the use of external data storage devices with your company's computers, such as flash drives, mp3 players, mobile phones, HDD devices and other gadgets that could potentially transfer dangerous files to your company's network. Good, lockable [USB blockers](#) are now out in the market to cover USB terminals, thereby protecting a computer when being left unattended for extended periods.

Taking care of information security is a primary concern, and companies should not take any chances. As technologies become more sophisticated, companies should readily adapt before their data can be exposed to any potentially harmful software. For more information on IT security call [All Covered](#) at 866-446-1133.