Understand the risks of cyber crime, says DRS director

Not a day goes by without the headlines being littered with stories about stolen credit card data, massive data breaches and similar. Most businesses, whether or not they know it, have suffered a breach and many individuals have fallen victim to cyber crime at one point or another.

Image: www.freedigitalphotos.net

To prevent this from happening, understanding what the risks are is the first step, says Jayson O'Reilly, Director of Sales and Innovation of DRS.

"It is impossible to imagine a world without internet or PCs," he said. "For the running of our day-to-day lives, these are essential. Because of this, cyber security affects us all, and knowing how to protect our data and avoid falling victim to these sorts of attacks is crucial."

He said that the range of risk is wide - from malware that can delete your data or even your entire system through carefully planned intrusions, or threats that take hold of your machine in order to attack other machines or commit DDoS attacks, to the theft of your personal data, which could result in financial losses - the risks are many and there is no such thing as total protection.

Identifying the risks

"However, identifying the risks is the first step. The first risk is the hackers or 'threat actors', the individual or groups of technically skilled criminals, who write code and attempt to infiltrate your systems. They use vulnerabilities or loopholes, exploiting them for their own nefarious purposes."

The code they write is called malware, or malicious code, which consists of all software that carries out the attackers' wishes. "Malware can be divided into several sub-categories: Trojans, worms and viruses."

Trojans, dubbed from the famous Trojan Horse, are not the same as worms and viruses as they do not independently replicate themselves. These programs pretend to be performing a specific function, but have a back door into the infected machine. Through the back door, cyber criminals have access to the machine and all its data, and can use these tools to steal banking credentials and other such information without the user noticing.

Worms, said O'Reilly, come in several forms too. Unlike viruses, which attach themselves to executable files, worms spread by transferring themselves via networks or other machines. "Network worms, email worms, peer-to-peer worms, IM worms are the main types of worms spread by cyber crooks."

Viruses

Viruses also replicate themselves in an attempt to spread to other machines. "In order to do this, they attach themselves to other files or embed themselves in the boot sector of data carriers. Often, they secrete themselves onto a computer via exchangeable media, such as flash drives, external drives or via the Web."

Viruses can attach themselves to several different elements of the operating system and can carry out their functions using a broad range of channels. "Viruses also have several different types, namely boot sector viruses, file viruses, multipartite viruses, companion viruses, macro viruses, stealth viruses and rootkits, polymorphic viruses, and email viruses."

O'Reilly said that there is no silver bullet, but practising 'safe' behaviour, such as not opening suspicious attachments or clicking on dodgy links, is a good start. "A good anti-malware solution is also a must. Make sure you keep it up to date and patch as soon as possible."