Companies unprepared for cyber attacks

Channel Islands' companies are at risk of incurring significant expense dealing with the aftermath of a cyber attack.

As a UK government-commissioned survey reveals the number of cyber attacks hitting businesses has soared in the past year and it is discovered that international cyber terrorists are specifically targeting Jersey, Rossborough and Next Generation IT are advising companies not to be complacent.

'Cyber criminals are becoming increasingly sophisticated and companies are more at risk than ever of having their cyber security compromised,' said Ian Stewart, managing director of Rossborough Guernsey.

'Keeping electronic information safe and secure is vital to a business's bottom line and no sector is immune from attack. The information that every company has stored can have a financial value and companies shouldn't underestimate the cost of rectifying an attack.'

Mr Stewart said that there was a misconception that traditional liability products address internet exposures but that liability for loss of customer or employee data was not typically covered under a corporate insurance policy.

'Some existing business insurance policies that offer general liability and director and officer liability may provide a measure of coverage for those areas but most companies will only discover if there are any gaps in what is and what isn't covered after an attack,' he said.

'Businesses can protect themselves and cyber liability insurance offers cutting-edge protection for exposures arising out of all forms of electronic communications. It addresses the first and third-party risks associated with e-business, the Internet, networks and informational assets, and can be built on a modular basis to suit any business needs.'

The Information Security Breaches Survey, commissioned by the Department for Business, Innovation and Skills, found some of the incidents caused more than £1m. of damage. The survey showed 87% of small firms experienced a security breach last year, which was a 10% increase on 2011, and 93% of large organisations had also been targeted. Affected companies experienced 50% more attacks on average than a year ago.

Next Generation IT director Jason Connolly said companies can take some very simple steps to minimise the risk of a cyber attack.

'The most likely cause for an attack is having weak passwords. A recent study found that the top three most commonly used passwords were password, 123456 and 12345678 which really presents no challenge for a hacker, regardless of whether they are targeting you for a specific reason to either damage your reputation or for financial gain or are simply being malicious,' he said.

'Companies need to have a well-maintained system which meets industry best-practices for securing their system, particularly regular patching. One of the most important measures is to carry out regular health checks to ensure any potential breaches are detected, investigated and corrective actions are taken to remove any infection and fix any weaknesses to minimise damage to the company.'

Mr Connolly said that as more and more business was carried out over the internet this had increased the odds of an attack.

'People often remotely access their work systems over the internet, but do not always take adequate security precautions, for instance accessing from internet cafes or home computers which are used by others, and will often have malware on them,' he said.

'Adding an additional layer of security with two factor authentication can help, and only remotely accessing from a non-shared PC or laptop is highly recommended.

'Cyber attacks are becoming increasingly sophisticated but if companies take a step back, look at themselves from the outside to see what information they have that might be valuable, take preventative steps and carry out regular health checks, then they will have made significant progress in minimising the risk.'