CYBERRISKS&LIABILITIES_

Defining, Identifying and Limiting Cyber-crime

A vast amount of information is now stored on computer servers and databases, and it's growing every day. Because that information has great value, hackers are constantly looking for ways to steal or destroy it.

Cyber-crime is one of the fastest growing areas of criminal activity. It can be defined as any crime where:

- A computer is the target of the crime
- A computer is used to commit a crime
- Evidence is stored primarily on a computer, in digital format

Understanding the various types of cyber-crimes can help identify and plan for a potential cyber-crime against your firm.

Computer Intrusions

It is a crime to gain unauthorised access to a computer system. There are several different offences that can be characterised as unauthorised access or computer intrusion, some include:

1. Obtaining national security information
2. Compromising confidentiality
3. Trespassing in a government computer
4. Accessing to defraud and obtain value
5. Damaging a computer or information
6. Trafficking in passwords
7. Threatening to damage a computer

Types of Computer Intrusions

Computer intrusions can come from an internal source, such as a disgruntled employee with an intimate knowledge of the computer systems, or an external source, such as a hacker looking to steal or destroy a company's intangible assets. The hacker can use a host of different means to try and steal or destroy your data in the following ways:

- Viruses—A virus is a small piece of software that attaches itself to a program currently on your computer. From there, it can attach itself to other programs and can manipulate data. Viruses can quickly spread from computer to computer, wreaking havoc the entire way. Email viruses became a popular method for hackers to infect computers in the late 1990s. These viruses were triggered when a person downloaded an infected document. When the document was opened, the virus would send that document to the first few recipients in the person's email address book. Some email viruses were so powerful that many companies were forced to shut down their email servers until the virus was removed.

- Worms—A worm is a computer program that can copy itself from machine to machine, using a machine's processing time and network's bandwidth to completely bog down a system. Worms often exploit a security hole in some software or operating system, spreading very quickly and doing a lot of damage to a business.

- Trojan horses—Common in email attachments, Trojans hide in otherwise harmless programs on a computer and, much like the Greek story, release themselves when you're not expecting it. And also like the story, the computer user has a part in letting the Trojan into the system. Trojans differ from viruses in that they must be introduced to the system by a user. A user can knowingly or unknowingly run an .exe file that will let a Trojan into the system.

- Spyware—Spyware can be installed on a computer without the user ever knowing it, usually from downloading a file from an untrusted source. Spyware can be used by hackers to track browsing habits or, more

importantly, collect personal information such as credit card numbers.

- Logic bombs—Logic bombs are pieces of code that are set to trigger upon the happening of an event. For example, a logic bomb could be set to delete all the contents on a computer's hard drive on a specific date. There are many examples of disgruntled employees creating logic bombs within their employer's computer system. Needless to say, logic bombs can cause serious damage to a company's digital assets.

- Denial of Service (DoS) and Distributed Denial of Service (DDoS) Attacks—DoS and DDoS attacks are used to send an overwhelming amount of data to a target server, rendering that server useless. A hacker does this by gaining control of several or more computers and then sends a large amount of data to a target server that it can't possibly handle. The result could be thousands or millions of pounds in lost sales for an online retailer and a complete loss of productivity for many businesses.

Limiting Intrusions

A computer intrusion could put your valuable digital assets at risk. That's why your company should have the following measures in place to limit computer intrusions and protect your assets:

- Firewalls—Firewalls are pieces of software that control the incoming and outgoing network traffic on a computer system and decide whether it should be allowed through or not. Most computer operating systems now come with a preinstalled firewall for security. While they are not the be-all end-all of preventing intrusions, they are a reliable start.

- Routers—Routers are pieces of hardware that keep unwanted traffic out of a computer system. They differ from firewalls in that they are standalone devices that must be bought separately–they are not included in an operating system.

- Antivirus programs—As their name implies, antivirus programs are designed to catch and eliminate or quarantine viruses before they can harm a computer system. Antivirus programs run in the background to ensure your computer is protected at all times. While they are updated frequently, they may not catch the newest viruses that are floating around.

- Policies—Every company, no matter its size, should have policies in place to educate employees on the dangers of computer intrusions and ways to prevent them. Make sure your employees know not to open, click on or download anything inside emails from untrusted sources. Employees with an intimate knowledge of the company's computer network should also be alerted of the potential consequences of hacking into the system.

- Common sense—Everyone claims to have it, but if that were actually the case, many viruses, worms and Trojans would cease to exist. The simple fact is that everyone in the company needs to exhibit some common sense when using a computer. Encourage employees to disregard emails with subject lines and attachments that seem bogus or too good to be true.

Review Your Risks and Cover Options

A computer intrusion could cripple your company, costing you thousands or millions of pounds in lost sales, damages and sanctions. Contact us today. We have the tools necessary to ensure you have the proper cover to protect your company against losses from computer intrusions.