Cyber Crime Explained

a Plain English Guide for UK businesses

jmglendinning
Insurance Brokers

Cyber Crime and Cyber Security have become big news in recent years. That's because Cyber Crime has continued to increase and is now a serious consideration for businesses of all sizes. This guide explains just how big a problem it is, and gives you some pointers as to how to minimise the risks your business faces.

What is Cyber Crime?

Cyber Crime is simply illegal activity, carried out predominantly through the use of a computer on a network. This would include such things as an unauthorised person hacking in to your network to access customer data, or hacking your website.

Some Cyber Crime is carried out for personal gain - for example, a hacker might look to gather data so that they can extort money from your competitors or fraudulently use payment details or passwords from your database.

On the other hand, some are carried out purely out of malice, or because a hacker knows of a certain weakness in your systems. For example, they might take down your website, or target you because you are using an outdated browser, and use the weakness to infect your systems with a virus.

What is Cyber Security?

Cyber Security is the body of technologies, processes and practices designed to protect networks, computers, programs and data from attack, damage or unauthorized access.

Or, to put it more plainly, it's the systems and processes you have in place to protect your electronic assets like your company's IT network , your data (be it stored within your network or externally) and even your website.

Cyber Crime is big news because it is on the increase – let's look at some statistics....

Just how big a problem is Cyber Crime?

These figures show just how big a problem Cyber Crime has become, right across the world. Whilst most of the headlines have focused on attacks against household name companies, businesses of all sizes are at risk.

£21 billion

The estimated cost of Cyber Crime to UK businesses in 2014

(Source: InfoSecurity Magazine)

42.8 million

Estimated number of worldwide cyber security incidents annually

(Source: PwC Global State of Information Security Survey)

43%

of UK Companies have suffered a breach

(Source:Experian Data Breach Resolution Survey)

56 million

The number of credit cards put at risk by ONE security breach from US Retailer Home Depot

(Source: InfoSecurity Magazine)

80%

of UK Cyber incidents could have been avoided through simple system and network 'hygiene'

(Source: National Audit Office,)

51%

of individuals will take their business elsewhere if their information is compromised

(Source: InfoSecurity Magazine)

So, Cyber Crime is a risk that can't be ignored, and next we look at how your business could be affected if you were to suffer a security breach....

How could Cyber Crime affect you?

Reputational Damage

If your customers' information was put at risk as part of a breach, it's essential that you tell them as quickly as possible, especially if sensitive information like passwords or credit card details were at risk. Once a breach has occurred, all you can do is limit the hit to your credibility, and notifying your customers immediately will show that you are taking the matter seriously.

Financial Costs

Ensuring that you don't get breached again can be costly. To start with, you may need a forensic examination of your systems to find what caused the breach. That could then highlight the need for upgrading your IT infrastructure and security. Preventing cyber security breaches is often much cheaper than recovering from one.

Loss of Customers

As well as the direct costs of fixing any security flaws, the damage that a data breach does to customer relationships can also be extremely costly. Whilst there are no definitive figures on customer defections after a breach, initial research by HyTrust in the USA suggests that more than half of consumers will take their business elsewhere if affected by a cyber security breach.

Loss of time and focus

As if all of the above were not enough, reacting to a cyber security breach can also tie up the time and resources of your people . Worse still, it will usually be your most senior people that need to be involved. That takes their focus off their day job, so they potentially miss out on other opportunities. This is yet another hidden cost of poor cyber security.

How can you help avoid a Cyber Security breach?

You must remember that there are no guarantees– cyber attacks have hit large corporations, so it can happen to anyone. However, there are plenty of steps you can take to reduce your risks, and eliminate some of the vulnerabilities that criminals will look to target.

- **Wifi networks –** Encryption methods have changed considerably since the early days of wifi networks – if you are using WPS encryption, your network could be highly vulnerable. Some companies also have a relaxed attitude to letting staff connect their own devices to the company wifi, which can increase risks.

- **Data usage by suppliers –** Do you pass data on to suppliers for marketing or other purposes? It is important to consider how secure their networks are, or whether you could find safer ways to share data with them.

- **Use of external storage devices –** Do your employees use memory sticks, internal hard drives or other devices? Portable devices can easily be lost or stolen, so ensure that use of such devices is limited to staff you can trust.

- **Software downloads –** Attacks can start off through people agreeing to download new or updated software, which often appear genuine Give your staff clear instructions on what they can and can't download. You may want to block non-IT staff completely from downloading updates.

- **Updating of browsers and other software –** Having said the above, genuine updates and downloads are needed regularly. Web browsers, and anti-virus software are just two examples of software that should be kept updated. Over time, hackers will discover and exploit weaknesses in software, and any updates are usually aimed at addressing these weaknesses, so although they may be time-consuming, they are important.

For more information including many free resources, visit www.cyberstreetwise.com and www.actionfraud.police.uk

What do you do if you suffer a Cyber Security breach?

If your business was hit by a Cyber Security breach, would you know what to do? If you don't, you're not alone – many business owners and managers wouldn't, so here's a quick guide to how you should respond, based on advice from the ICO (Information Commissioner's Office).

1. **Report the incident–** Action Fraud is a specialist division of the Police, and will receive reports on actual or attempted online fraud and cyber crime. Details can be submitted through their website – www.actionfraud.police.uk

2. **Notify any customers involved immediately** – this will mean a hit to your credibility in the short-term, but by this stage, damage limitation is key. Your customers would rather find out now that their data has been breached, rather than later on when – for example – their passwords or credit cards may have been used fraudulently.

3. **Notify regulators or other relevant bodies –** If you operate in a regulated industry, or are registered as a Data Controller with the Information Commissioner's Office, you should notify the relevant authorities of the breach.

4. **Investigate the causes –** If you use an external IT company, start by notifying them, and they will usually be able to guide you through the process, which may involve drafting in some specialist expertise.

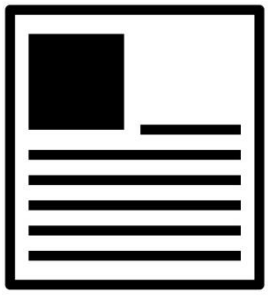
5. **Get outside help –** If you manage your IT in-house and have no-one to help you through the process, you may need to consider external support. The growth of cyber crime has led to the emergence of specialists offering support after the event. By searching online for "Cyber Security Incident Response" you will find many specialists in this field.

6. **Make any necessary changes to IT processes –** By now, whether you've worked with your IT provider or a Cyber Incident specialist, you should know what you need to do to tighten up your security, so you must agree an implementation plan as to how and when everything will be put in place.

Remember – doing nothing is not an option. Cyber attacks happen because of vulnerabilities. If you ignore the problems, they will not go away, and may even get worse.

How Cyber Liability Insurance can help

The growth of Cyber Crime has meant that Cyber Liability Insurance is now more commonplace, which in turn has helped make premiums more competitive for businesses of all sizes.



We can arrange Cyber Liability Insurance with a variety of specialist insurers. The exact nature of the cover will depend on the individual insurer, but here's an overview of the cover you might expect to see on a policy:

- **Cover for costs incurred in recovering from the incident –** this includes costs for forensic examination of your systems, legal advice, notifying customers and support such as credit monitoring of affected customers.
- **Cyber business interruption –** your loss of income resulting from the breach. This would typically be excluded from your standard business interruption policy.
- **Privacy protection –** this covers claims made against you by customers affected by the breach, as well as costs associated with any regulatory investigations.
- **Hacker damage –** this pays for repair and restoration of your website, programs or data after malicious damage from hackers.
- **Cyber extortion** – if hackers try to hold your business to ransom, this section of the policy provides specialist advice and can cover the cost of the ransom.

Here's how to get a quotation from us for Cyber Liability Insurance…

Talk to us for a quotation

Cyber Liability Insurance can be an important part of your efforts to protect your business against Cyber Crime.

Cover needn't be expensive, with premiums starting from as little as £400 (plus Insurance Premium Tax @6%).

For a quote and some simple advice on Cyber Liability Insurance speak to your nearest office – contact details can all be found below.

Guiseley, Leeds
Elmwood House
Ghyll Royd
Guiseley
Leeds
LS20 9LT
Tel: 01943 876631

South Yorkshire
Bullhouse Mill
Lee Lane
Millhouse Green
Sheffield
S36 9NN
Tel: 01226 761195

North East
1 Park Road
Gosforth Business Park
Newcastle upon Tyne
NE12 8DG

Tel: 0191 256 0957

www.jmginsurance.co.uk
info@jmginsurance.co.uk

Call us today for professional, friendly advice on any aspect of your Business Insurance.

jmglendinning
Insurance Brokers