OVAL
Insurance Broking

Insurance Solutions with extra byte

Oval Technology and Telecommunications June 2012

Cybercrime - its consequences and how to protect yourself

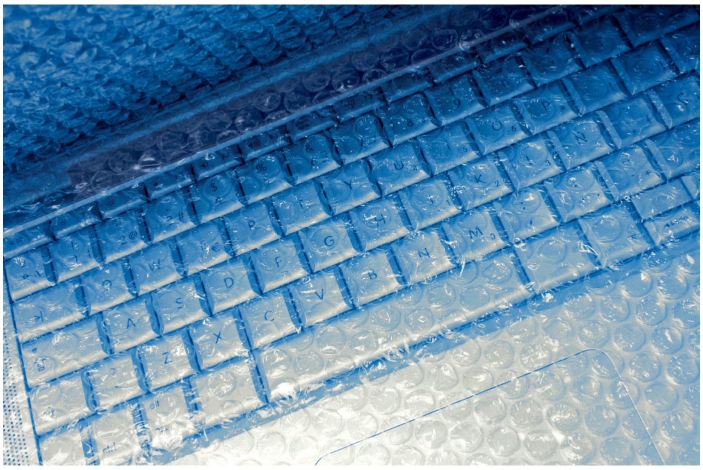
We are riding the wave of digital development, eager to embrace new technologies that can improve our lives and our businesses. Whilst our enthusiasm and uptake for new technology is exponentially growing, there are also those out there who are looking to exploit it. Our desire for the new can often bring with it naivety, which makes us vulnerable to the new breed of criminal – cybercriminals. This article will explain how the risk landscape has changed, what the emerging threats to your business are, why existing insurances might not respond and what steps you can take to protect yourself.

Cybercrime is different to other forms of traditional crime in that the use of the internet means that criminals do not have to be physically present at the scene, or even in the same country as the victim. This makes cybercrime much more difficult to detect and often this can be months after the initial attack. The perpetrators are often in different jurisdictions, where laws are lax and there are not the resources to investigate, or a willingness to prosecute.

This perpetuates an environment that favours the criminal, they are entrepreneurial, resilient and stay one step ahead of the security measures companies invest in. Even when steps are taken to protect IT systems with anti-virus security software, viruses and hacking techniques are constantly evolving, making the software redundant almost immediately. Criminals are more motivated to commit crimes than the victims are to prevent it.

It is small wonder then, given the low risk of being caught, the minimum effort required and the seemingly endless opportunities, that cyber attack is being seen by most governments as a bigger threat than terrorism.

Whilst the headlines in the news are usually reserved for the big names or government organisations, this does not mean you can afford to be complacent. Increased spending by large enterprise on IT security and staff awareness training has diverted the attention of criminal organisations to target medium and even small businesses.



"Know thy Enemy"

So who is behind all this? The culprits of these attacks can be broken down in to five distinct, but often overlapping categories;

- Irritants
- Ideological
- Financial
- Political
- Human

Irritants: These are often individuals who can cause low level damage through internet vandalism or pure curiosity. Sometimes referred to as "Script Kiddies", they are usually only interested in the bragging rights of getting access and leaving their mark, a bit like the use of graffiti to "tag" property. These hackers get in, leave their mark and get out. As individuals they are at the low end of the damage scale, however as a collective they can be more dangerous, forming loosely connected hacking groups such as Anonymous.

Ideological: These are hactivists with a socio-political agenda, targeting companies who they believe are contributing to unethical, or irresponsible behaviour. Attacks are often targeted with the intention of causing damage and pain to a business. Typical examples include LulzSec or Anonymous teaming up with the Occupy movement and threatening to attack financial institutions. Due to the rise of social media sites, such as twitter, attacks can be quickly coordinated between members and can be impossible to predict or prevent.

> "There are only two types of companies, those that have been hacked and those that will be."
> Robert Mueller, Head of the Federal Bureau of Investigation

Financial: This is probably the area where there is the most activity and can be split between criminal activity and industrial espionage. The virtual black market for trading in stolen data is driving demand, and even the simplest of personal data can be traded for a profit. A joint report issued by the UK Cabinet Office and Detica in 2011 suggested cybercrime is costing the UK private sector £21 Billion each year.

Industrial espionage often targets companies' valuable intellectual property (IP), whether this is a theft of trade secrets, a direct attack on an organisations' automated processes by a competitor, or an individual looking to make a profit.

In a 'One Show' report for the BBC it was estimated that theft of IP has cost UK companies £ 9.2 Billion. A well orchestrated attack on a company can wipe out its research & development pipeline for the next 15 years.

Extortion can also play a big part, where an attack does not even have to occur, the threat alone can be enough to make a company pay up.

Political: Individual countries are occasionally alleged to be directly or indirectly involved in attacks. Whether through electronic warfare such as the alleged involvement of the USA and Israel in the development of the Stuxnet virus targeted at the Iranian nuclear programme, or possible Chinese support of intellectual property theft. These types of attacks often require colossal effort and deep pockets which only national governments have access to.

Human: There is always the threat from within. This could range from disgruntled employees colluding with cybercriminals, a member of staff moving to the competition and stealing data on a USB stick, or the use of a companys' IT by a member of staff to carry out fraud. Whilst external attacks can require specialist skill sets or at least a large amount of effort, it is far easier to commit cybercrime when you are already inside.

Consequences of an Attack

Following an attack on your business, when you actually discover it, you are often faced with having to incur costs to repair and prevent future attacks. You are then left vulnerable to the claims from third parties for loss of their data, or failure to fulfil a contract. The consequences to your business can therefore be split into costs you will directly incur – first party losses, and those you have to pay to other people – third party losses.

First Party Losses

Costs and Expense – Immediately following an IT incident, funds are needed to correct the problem and deal with the consequences, such as:

- Forensics to discover the source of the incident
- The replacement of data lost or compromised
- A solution to fix the problem and prevent it happening again
- A penetration test of the affected network to ensure there are no other 'holes'
- Notification to clients who have had their data accessed
- Credit monitoring for clients affected
- Other costs required to comply with the appropriate regulator

In a recent report by Norton they estimated that the value of cyber crime is over US$380 Billion – larger than the global black market in marijuana, cocaine and heroin combined.*

*Source: Norton Cybercrime Report 2011

Fines and Penalties – Currently the Information Commissioners Office (ICO) has the power to levy up to £500,000 in fines against a company for loss of personal data. If you are doing business in the USA these awards can be even more substantial.

Loss of Intellectual Property – If a secret is worth having then it is worth stealing, not necessarily by the direct competition, but by a third party who recognises the opportunity of stealing it to sell on to the highest bidder. Lost IP can destroy a company's research & development pipeline and future trading position.

Downtime – When your IT system is compromised this can lead to server downtime, while the cause of the breach is discovered, fixed and prevented from happening again. When you are reliant on IT for day to day processing, this can lead to substantial trading losses.

Brand and Reputational Damage – Much of the damage caused following an attack on an IT system can be indirect, materialising through loss of reputation and damaged brand, leading to lost sales and reduced share price. If a business is unable to supply its goods, customers will look elsewhere for alternative suppliers and may not return once the system is back up and running.

Third Party Losses

Legal Costs and Awards – Loss of data, whether electronic or stored traditionally on paper can lead to legal action against an organisation. Not only does this mean incurring legal costs, but also awards for cost and damages. Your customers might also look for compensation for your inability to fulfil their contracts due to IT failure.

Physical Loss or Damage – Where there is an element of automated manufacture or process there can be a very real threat to property and possibly life when systems fail. Systems which operate industrial processes (such as car manufacture) can be just as much at risk as any computer network. The likelihood of attack is high - after the public sector and the chemical and pharmaceutical industries, the manufacturing sector is the third most likely industry to be attacked.

(Source: Symantec Intelligence Report: Nov 2011)

Insurance Covers – Issues and Solutions

The direct costs of fixing, repairing and monitoring an IT loss, the fines and penalties, potential lawsuits and legal costs coupled with lost income, missed income opportunities and indirect reputational or brand damage can all result in lost income, as well as a hefty bill.

So why is it unlikely that your current insurance policies will respond?

Property Insurance: Traditional property policies such as commercial combined, only usually cover the physical assets. The losses described in this document are to the intangible assets and therefore not covered by these policies. Additionally there are often standard exclusions for virus, hacking and other IT risks.

Business Interruption: As there is no physical loss or damage, the insurance policy will not respond to claims for business interruption/loss of income, or for increased cost of working.

Computer All Risks Package: Again this type of policy covers the cost of repairing the physical assets, such as hardware following physical loss or damage. Cover can be extended to include the cost of reinstatement of data and increased cost of working, but once again these policies often carry standard virus and hacking exclusions, which would remove the cover required for intangible asset risks and losses.

Liability: A public and products liability policy only indemnifies for bodily injury and property damage losses. As data is not physical property, it would be unlikely to respond to a third party claim of privacy breach or financial loss. It might be possible to make a claim under mental anguish, or possibly trespass under this policy, but this is an uncertain course of action.

Professional Indemnity(PI)/Errors and Omissions(E&O): Whilst professionals might carry 'PI' cover and other industries some form of 'E&O', these will only provide cover for losses that occur in the ordinary course of your business. If negligence results in the theft of data, this could leave you with an uninsured loss. An example could be a hacker using your network to gain access to a third party network to perpetrate a theft. In addition, there would be no cover for claims brought about by your own employees losing data. These policies also carry the standard virus and hacking exclusions and there would be no first party protection.

Crime/Fidelity Guarantee: These policies provide for financial loss of tangible assets as a direct consequence of actions of an employee, or where suitably extended an external third party. These polices are tailored to look after the insured's first party losses of money, securities or other tangible financial property (such as stock), or those of clients in their care, custody or control. Whilst there could be cover for online theft of money if suitably extended, there would be no protection for theft or destruction of intangible assets such as data, or the consequential loss of profits that follows from such an incident. Likewise, there would be no third party cover for allegations of financial loss.

Summary

Whilst it is possible to extend policies to cover a range of "what if's" by endorsement, it is a "risky" strategy. A far safer approach is to have the correct insurance policies in the first place, which will provide wider, more reliable cover.

What are the insurance solutions available?

The good news is that it is not all doom and gloom and there are viable and cost effective policies that can protect you from these emerging perils and consequences. These policies can be either package policies that also include the material damage and liability aspects, or more stand alone polices that compliment your existing insurance.

These insurance policies cover the essential first and third party exposures you may have.

First party covers include:

- Loss of or damage to digital assets (such as data or websites)
- Non physical Business Interruption
- Additional expenditure costs (forensic testing, security consultants)
- Customer notification costs and credit monitoring
- Costs of complying with the regulator
- Where permissible by law, any fines and penalties
- Extortion
- Public relations costs
- Theft of intellectual property pursuit costs
- "Cyber Terrorism"

Price Waterhouse Cooper's (PWC) 2011 report into security breaches noted that 93% of large organisations and 76% of small business have had a security breach in 2011, this is up from 35% of companies overall in 2008.* PWC advised in their report that the average cost to a small business is £15,000 – £20,000 and between £110,000 – £250,000 for a large organisation.

*Source: PWC's Information security breaches survey Technical report

Third party covers include:

- Privacy breach claims for lost data
- Accidental damage to third party networks
- Network security failure
- Libel and slander
- Infringement of intellectual property costs

Oval had experience in assessing the cyber risk and insurance profile of its clients, and tailoring a solution that suits the requirements of different organisations from the wide number of insurers available in the market

As a top UK insurance broker, Oval Insurance Broking have the practical and professional expertise that has made us the insurance partner of choice for many, providing peace of mind for your insurance requirements, as well as a continuing analysis of the insurance market and trends impacting UK businesses.

Would you like to talk?

If you would like to discuss your need for cyber risk protection, or your risk and insurance needs in general, please contact:

Richard Hodson on 0207 422 5600,

or drop him an email at
richard.hodson@theovalgroup.com

Alternatively, please speak to your usual Oval representative.

Oval Insurance Broking Limited
Registered Office: 9 South Parade, Wakefield, WF1 1LR
Registered in England No: 01195184
Authorised and regulated by the Financial Services Authority