Risk Solutions

Cyber security for small and medium-sized businesses

A guide to loss prevention

HSB Engineering Insurance

Munich RE

Organisations of all sizes are vulnerable to cyber security breaches. However, they can often significantly underestimate the threat of cyber risks and, following a breach, be unprepared to deal with the resulting financial and/or reputational damage. *74% of small businesses in the UK suffered a cyber security breach in 2015, with the average cost of those breaches reaching £75-£311k (£65-£115k in 2014).

Most businesses, large and small, rely on computers and mobile devices to collect and store information; from details on customers and employees, to suppliers and competitors, to name a few. More often than not, these devices are connected to the Internet.

Cyber security is about protecting both computer equipment and, more importantly, information stored on that equipment from unintended or unauthorised access, change or destruction; either internally through deliberate action or employee error, or from external threats (such as hackers) that use the Internet to gain access. Common problems include employees inadvertently exposing IT network to malicious software (or malware; simply by plugging in external devices and USB memory sticks), opening infected emails or even using an unsafe website infected with malicious code.

Consequently, it is vitally important for all businesses to take steps to ensure that their systems and data are secure.

A guide to loss prevention

This guide has been prepared to give helpful advice on how to protect organisations from cyber threats, using a 10-step guide developed as best practice by the Communications Electronics Security Group (CESG), the information security arm of the UK Government.

Storing data

Businesses store data about various groups - customers, suppliers, employees, products and services - on computers and storage networks. Authorised users have come to expect easy and near instantaneous access to this data at all times, which presents significant challenges when it comes to data security. Being able to rely on the security, accuracy and quality of that data can often be taken for granted.

All UK businesses have a mandatory obligation, backed by UK legislation (Data Protection Act 1988 and the UK Computer Misuse Act 1990), to protect personal information relating to individuals from all cyber risks and threats; such as theft, erasure, corruption, loss or unauthorised access. Enforcement of these responsibilities in other countries is defined by statutes, including various 'jurisdictional' data protection and computer misuse acts. Under current UK legislation, breaches of such data can, in serious cases, lead to substantial fines.

Potentially more damaging is the reputation of a business, which can be affected where inadequate security or negligent practices are to blame.

A business's reputation can take years to build, but only moments to destroy.

Robust data backup regimes are still very important. With the advent of the Internet, additional data storage and backup methods have become available. This includes cloud storage which is accessed via the Internet and is not necessarily running on the business's own IT network. For this reason, much of the data used by businesses to trade today is replicated across, and accessible from, multiple sources. Consequently, the data is more vulnerable than ever to attack by third parties who can exploit poorly-protected Internet connections and weak security regimes to gain unauthorised access to business-critical information; often with malicious intent.

Internal security breaches

Unauthorised access to IT networks and stored data may occur as a result of an employee making an innocent error, such as forgetting to log off from a secure computer process, making a payment transaction or accounts processing operation, or simply forgetting to log out whilst they are away from their computer for a period of time.

Security breaches can also be deliberate and conscious actions, such as sharing a log-in identity, password or swipe card. Such a security breach may involve transferring information to/from the business's IT network via removable devices (such as a USB memory stick), but can also involve exporting/importing unauthorised information, software or malware via the Internet.

Where an action results in the loss or corruption of data, it is considered a computer security or cyber breach; regardless of whether it resulted from an innocent error or malicious act. As such, businesses must install robust systems for controlling access to its computer, software and data systems. Employees should receive cyber security training so they are made aware of the risks and how to mitigate them.

Most employees do not require access to all levels of a business's IT network at all times. Implementing a password log-in system to allow employees access to only the information and software they require to perform their jobs are just some examples of basic measures that can be taken.

Access to systems may also need to extend to Internet-based resources, including use of email and Internet browsers; in which case, further measures should be considered to restrict access to only the on-line resources required.

*2015 Information Security Breaches Survey – Department for Business Innovation & Skills

It is important for businesses to promote awareness of computer cyber risks and threats throughout their organisation, and for employees to be aware of their own responsibilities for data security at all times. A clear statement of company policy, supported by ongoing training programs to educate employees in effective cyber security, is something all businesses should implement.

Internet risks

Today, most businesses use the Internet for basic business activities, including sales and marketing, electronic trading, and to communicate with customers, employees and suppliers. eCommerce trading, whilst considered positive with certain opportunities and benefits, can also introduce additional risks and threats to a business.

Every day, businesses around the world experience cyber attacks on their IT networks via their Internet connections. Typically, these are attempts to access information, steal money or sometimes just deliberately disrupt the running of the business for no particular reason. Cyber attacks can take the form of a malicious software virus attack (malware), unauthorised access (hacking), and Internet hi-jacking or disconnection (denial of service/ distributed denial of service or DoS/ DDoS). These attacks almost always impact on the ability of the business to trade normally and can seriously affect a company's profitability.

The first line of defence for any IT network should include anti-virus software for checking all email traffic sent to and from the business, and firewalls to protect against unauthorised access via the Internet.

In addition to automated programs, businesses should also have a clear internal policy to discourage employees from random Internet browsing using business IT equipment, thus avoiding fraudulent websites where viruses and malware can often lurk.

10 steps to cyber security

In addition to statutory requirements set out in UK data protection and computer misuse acts, the UK Government has published guidelines on information systems risk management. CESG, the information security arm of Government Communications Headquarters (GCHQ), has developed 10 steps of best practice which, if implemented, will help businesses worldwide defend against cyber risks and threats. The guidelines will help businesses develop a good foundation for effective business information risk management, with particular emphasis on network and Internet threats and vulnerabilities.

The 10 steps are summarised as follows:

1. Develop an information risk management regime and risk aware culture

It is important that cyber risk management policies are imposed with the full authority of owners, directors and managers of the business.

Even in small organisations, it is desirable to have one person whose role includes responsibility for information security and taking steps to limit the business exposure to cyber risk.

Cyber risk is not just a problem for IT departments and technical employees, and a cyber risk-aware culture can only be effective in an organisation if there is a clear policy and commitment defined by the owners and leaders of the business.

2. User education and awareness

As well as top down commitment from the owners and leaders of the business, another key component is a bottom-up commitment by employees. All levels of employees requiring access to business IT equipment to undertake their jobs must understand precisely what their cyber security roles and responsibilities are.

Cyber security policies are best defined as a written policy prepared by key managers for implementation in the working environment. It is essential to educate and train existing employees and new starters to make sure they understand the defined cyber security policy, and to obtain their commitment to observe it during the course of their day-to-day work.

It is also advisable to have regular revision and re-training sessions to ensure user awareness and responsibilities are maintained on an ongoing basis, and to implement any security changes that may be required as a business grows; especially if its use of computers and mobile devices increases.

3. Incident management

A business that is reliant on IT equipment and information systems should establish a pre-defined plan of action so that all employees know what to do in the event of a cyber-security incident. This plan will generally form part of an overall business continuity plan (BCP) and should include, as a minimum, first response and escalation procedures for information systems disaster recovery.

From time to time, the response plan should be practiced (in the same way businesses practice fire drills) to ensure it is adequate and fit for purpose.

All employees should know the name and contact details of the person with responsibility for cyber risk security for the business and be able to contact them quickly, preferably in person or by phone, to notify them that an event has occurred (or a near miss avoided).

As deliberate breaches and malicious actions by employees can occur, the business should have a procedure in place to formally remove personnel in the event of misconduct and dismissal. In this scenario, access to the business's IT networks, both at the business premises and via the Internet, should be immediately prevented; typically by having their user account rights removed or suspended.

4. Home and mobile working

Home workers and employees equipped with laptops and smartphones are now a routine feature of most businesses today. These devices often operate independently of the fixed IT systems located at a business premises and can sit outside of any firewalls or virus defence software that protects a network. As a result, a specific mobile equipment cyber security policy should be in place. All employees must be made aware of their own responsibilities and be properly trained to comply with the policy. Typically, this includes implementing security procedures such as secure networking, which includes the use of encryption to ensure that sensitive business data is encrypted when accessed, stored or transmitted online, and is restricted to authorised users only.

Organisations should also be mindful that, at all times, it is essential to protect sensitive data whilst it is physically in transit or at rest. Devices such as business laptops and/or removable media (such as USB memory sticks) should not be carried casually or left in places vulnerable to theft.

All mobile devices that carry business information or can access the business's IT network remotely must be password protected and have their own free-standing anti-virus and firewall software installed. Anti-virus software should be configured to update automatically when mobile devices are connected to the Internet.

In the event that a mobile device is lost or stolen, the business owner should have a mobile device management solution in place whereby, as a last resort, all corporate data can be remotely wiped from the device.

5. Managing user privileges

As far as is practically possible, employee and third-party access to business computers and IT networks should be restricted to the minimum level required to undertake a job function or process a business transaction.

Privileged accounts (those used by systems and network administrators to gain wide ranging access to business computer systems and network controls) should be limited to as few key people as possible.

The person responsible for cyber risk security for the business should issue guidelines to users regarding the use of suitable passwords. Password changes should occur automatically (known as forced changes) at intervals appropriate to the level of access required, but more frequently for users who have access to sensitive accounts and information.

To ensure users have the correct level of access, network access (such as log-ins/log-outs, time online and other relevant activity) should be recorded (manually or automatically using software). Periodically, this information should be audited by a designated senior person or manager of the business who is able to interpret such information with discretion and in accordance with applicable legislation.

It should be kept in mind that company employees do have privacy rights. The responsibility for auditing such user information should, therefore, be strictly limited to senior personnel on a need-to-know basis.

6. Removable media controls

As far as is practically possible, businesses should limit the use of removable media such as USB sticks, memory cards, CDs and DVDs. Where such use is unavoidable, password protection should be used and media should be automatically scanned for viruses and malware before importing data to or from any connected business IT network.

7. Monitoring

Businesses with IT networks should consider installing network access monitoring and security software. This software has the ability to continuously monitor connected business users on the IT network, as well as external connection requests made by users browsing or accessing business resources via the Internet.

Conditions can be defined in the monitoring software to raise alarms to business owners and managers in the event of unauthorised activity. If any issues are detected, this should be escalated and investigated by the person in the business responsible for cyber risk security.

8. Secure configuration

Preventing, detecting and limiting the effects of cyber risks and threats is heavily dependent on the business IT network's firmware and software being up-to-date, so it is important to ensure the latest security patches and bug fixes are applied. Hence, it is essential that there are defined procedures for applying operational and security patches and virus updates. It is usual to have a designated person who ensures that updates are reviewed and applied on a regular basis, and who keeps a written record or log.

Security measures and anti-virus systems must also be kept up-to-date to ensure their effectiveness against the latest threats which evolve almost daily. Most protection software is designed to update virus definitions automatically (provided there is a valid Internet connection) and will constantly scan for viruses and malware without disrupting the main computers and software applications.

Businesses should also compile a detailed inventory of all IT equipment and software, and should aim to establish a secure standard configuration for all existing and future IT equipment; as far as possible, each business computer configuration and user experience should be consistent. User access to the general business IT network then becomes easier to manage through centralised procedures, and makes it easier to deliver common software and anti-virus updates.

9. Malware protection

Anti-virus and malware protection software is usually the main defence against damage to IT networks and systems as a result of external threats from the Internet. Viruses are often carried as email attachments, or may be accidentally (or deliberately) downloaded via the Internet. They can also be loaded onto a business's IT network via internal network access points if removable media is used.

Scanning and monitoring for viruses and malware across the organisation information systems and networks must be a continuous process, running at all times. If a virus threat is detected, the anti-virus software can often neutralise it before it causes harm to the IT network, or at least will quarantine it so that it cannot spread throughout the IT network.

Automated virus and malware activity alarms should immediately notify the person responsible for cyber risk security for the business.

There should be an escalation strategy to isolate the virus from other computers and storage devices on the network as quickly as possible in the event that the anti-virus measures are not able to neutralise it automatically.

10. Network security

Organisations need to protect their IT networks and data storage against internal and external threats, whilst at the same time being able to connect to the Internet securely. To achieve this, the Internet-facing network perimeter should be protected by firewalls, which can take the form of software or hardware devices depending on the size of the network.

Internet-connected networks can further benefit from a perimeter network, a secure staging area between the organisation's internal secure network and the Internet. This adds an additional layer of protection by only exposing a small part of the network to the Internet.

Keeping your IT hardware physically protected

Whilst the security of stored data is an important consideration, it is also important to physically secure the IT equipment, hardware and infrastructure supporting that data.

If a company is dependent upon server-based IT systems, the server (or servers) should be located in a secure, self-contained room protected by a locking door (a simple key lock, combination lock or electronic swipe card, for example). The key holder/personnel access list should be restricted to only those employees who require access to the server room to undertake their roles. Contractors and visitors requiring access to the server room should be escorted at all times. CCTV may be used to monitor personnel going in and out of the room, or alternatively installed in the server room itself.

The location of a designated IT equipment room within a building is also an important consideration. Its location should preferably be within the deeper interior of the building rather than on the perimeter of the building. Also, upper floors tend to be more secure than ground floor locations. If the latter is unavoidable, the IT equipment room should preferably have obscured (or no) windows, or else have blinds fitted so that equipment cannot be viewed casually from outside the building.

If possible, IT equipment rooms should not be located close to plant rooms or primary/legacy water systems such as water mains, overhead water pipes, heating tanks and/or drain valves. If the latter are in close proximity, the IT equipment room should be fitted with a raised floor and there should to be a water escape route or drain sump installed. In areas susceptible to flooding, the positioning of IT servers and storage of equipment in basements should be avoided.

The temperature environment in which centralised IT server and data storage equipment operates is also an important consideration. Manufacturers recommend a strict range of operating temperatures. If the lower or upper operating temperatures are exceeded, equipment may not operate correctly and, in some cases, warranties and guarantees on the hardware can be invalidated. Temperature control is usually achieved using air-conditioning systems suited to the room and the heat loading of the installed equipment. Professional heating and ventilating design guidance should be sought in this regard.

Even so, air-conditioning systems can occasionally breakdown or be shut off accidentally. It is, therefore, recommended that separate and independent temperature monitoring systems are installed to provide an additional element of protection from such events. These typically inexpensive items monitor the ambient temperature in the server room and, should specified temperature parameters be exceeded, will activate local alarms and send alarm text messages/emails to appointed parties to enable them to take the earliest steps to investigate the issues and prevent damage. Some of the more sophisticated systems can even be set to power down the server to prevent damage, without the necessity for human intervention.

Protecting IT equipment assets from fire is also an important consideration, and there are a range of options that can be implemented. A IT equipment room should always have a 24-hour operational smoke and fire alarm installed to ensure earliest detection of any fire event occurring.

Handheld fire extinguishers/fire points should be located inside or immediately outside the IT equipment room. Fully automatic inert gas discharge systems tend to be installed in larger IT equipment rooms, which quickly suppress fire and smoke and limit damage to installed equipment.

Consideration should also be given to the quality of the electrical supply in the IT equipment room. A dedicated ring main supply can reduce the risk of electrical noise and harmonic interference from other non-IT equipment connected to the same circuit.

Dedicated electrical circuits can still be susceptible to mains-borne transients from lightning or grid switching (sub-station) events - use of electrical transient suppression devices is desirable. This is particularly of concern in factory and machinery operating environments, as well as larger commercial and office buildings in urban or industrial estate environments. These can be simple plug-in devices between an IT equipment's power supply and the mains, or may require professional electrician installation in primary and/or sub main distribution circuits supplying larger dedicated IT equipment rooms.

An Uninterruptable Power Supply (UPS) is a short term battery backup device which can help prevent damage to IT hardware in the event of a sudden loss of building power or grid power cut. Larger more sophisticated UPS models have the capacity to initiate a controlled power-down of all connected equipment, lessening the risk of damage and/or loss, or corruption of data. Some UPS models also incorporate built-in harmonics and transient protection of the type referred to above, but this is not true in all cases. Careful technical guidance on this aspect needs to be sought from the prospective vendor before purchase and installation to ensure the chosen UPS can cope with the applied electrical loading of the IT systems to be attached, and will provide the expected electrical protection benefits.

As well as protection of the key hardware in the IT equipment room environment, the resilience of the connections from the room to external networks in the same building, the Internet and cloud computing resources should also be factors for consideration. Redundancy in such cabling systems is desirable where possible, and key connection cables should be routed as far as possible to minimise the risk of physical damage.

In the work office environment, IT equipment - such as base units, printers, monitors and laptops - can be physically secured to desks using lock and cable-type systems, reducing the risk of casual theft for more portable items.

Loss example 1

Virus introduced via USB memory stick

A consultant engineering practice that used computer-aided design allowed employees to take digital drawings (which tend to be large files) to and from the business offices to work on their own computers at home. Although the business had anti-virus systems installed to protect the risk from virus infection via email and the Internet, it was not configured to automatically scan removable media.

An employee inadvertently brought a virus in from their home computer on a USB memory stick they had been working on. When the memory stick was plugged in at work, the virus was transferred to the business's IT network, causing the corruption and erasure of files. This resulted in many hundreds of hours of work being lost, at considerable cost to the company, before the virus could be isolated and neutralised.

If the business had its anti-virus systems correctly configured to scan removable media, it is unlikely the virus would have been introduced onto the business's IT network in the first place. At the very least, it would have been quarantined and prevented from causing damage to their business data.

Loss example 2

Password sharing

A small contracting business, with half a dozen computers on an Internet-connected IT network, was IT-administered in-house by the owner who had a limited knowledge of computing.

When a network user account was created, all employees were unfortunately issued with the same password which they were not necessarily required to change. Worse still, the common password provided users with access to all parts of the IT network, including business accounts and online banking.

Following a dispute with an employee over pay, the disgruntled employee was able to log into the company's bank account and transferred several thousand pounds to an unknown destination; significantly affecting the business's cash flow. There was strong suspicion over who had stolen the money, but because several people knew and used the same password, police were unable to prosecute. Although the employee under suspicion was dismissed, the money was never recovered.

The business owner should have made sure all users had a different password through a forced change at first log-on. In addition, only a senior and trusted credit manager should have had access to the accounts and online banking; in which case this loss could have been avoided.

References and guidance

Further guidance for businesses on cyber risks can be found in the following publications:

- Protecting small businesses from a data breach – HSB Engineering Insurance (www.munichre.com/HSBEIL/products/cyber-insurance)
- Cyber security: what small businesses need to know – Department for Business Innovation and Skills, HM Government (www.gov.uk/government/publications/cyber-security-what-small-businesses-need-to-know)
- Cyber Essentials Scheme – HM Government (www.gov.uk/government/publications/cyber-essentials-scheme-overview)
- Managing Information Risk – HM Government (www.gov.uk/guidance/managing-information-risk)
- A practical guide to IT security – Ideal for the small business – The Information Commissioners Office (www.ico.org.uk/for-organisations/guide-to-data-protection/principle-7-security/)
- UK Data Protection Act 1998 (or appropriate jurisdictional equivalent)
- UK Computer Misuse Act 1990 (or appropriate jurisdictional equivalent)
- The ISO27000 family of standards - designed to help manage security of assets such as financial information, intellectual property, employee details and third party information held. (http://www.iso.org/iso/home/standards/management-standards/iso27001.htm)

HSB-LCE-RGN-014 Rev: 0 Date: 20/10/2015