Data Security

What is Data Security?

Data Security is the means of ensuring that data is kept safe from corruption and that access to it is suitably controlled. The focus behind Data Security is to ensure privacy while protecting both Personal and Corporate data.

Why do I need to be concerned about Data Security?

You may be breaking the law under the Data Protection Act and you may be liable for prosecution. Security breaches may cause harm to the individuals they affect, they can also affect your company's reputation.

How to improve Data Security?

There is no single approach to securing data. There are however three clearly defined areas that must be considered together when looking at ways to secure data. These are:

1. The Security of the Data itself (Data Security)

In order to secure data, controls must be in place defining the locations where data resides, the mechanisms of data flow and who has access to the data.

There are a number of ways to do this:

- Have a central repository of all data (Server). This can give the utmost control of who accesses the data and provides the ability to back it up centrally
- Ensure that users who access the data only have the ability to view what they need to complete their work. Never give users more access than they need
- Reduce the amount of sensitive data that is taken outside of the company without adversely affecting your work
- Ensure that all mobile devices (smartphone, laptop, etc.) are password/PIN protected
- Ensure that all laptops that contain sensitive data have encrypted hard drives (or store sensitive data on an encrypted USB key)
- Ensure all users have strong passwords
- Ensure that all computers/laptops are shut down when not in use, as opposed to putting them into sleep or hibernation modes

2. The Security of your IT Network (Network Security)

In order to ensure data security you must secure your IT network from external threats. The majority of these threats originate from outside of your network through the internet.

The most common threats include:

- Viruses, Worms and Trojan Horses
- Spyware and adware
- Zero-day attacks, also called Zero-hour attacks
- Hacker attacks
- Denial of service attacks
- Data interception and theft

Network Security usually consists of multiple components, that when working together improve your security. These components include:

- Anti-Virus and Anti-Spyware software
- Email filtration (SPAM) services
- Firewalls, to block unauthorised access to your network
- Intrusion prevention, to identify external threats
- Virtual Private Networks (VPNs); to provide secure remote access to your network

3. The Security of your IT Equipment (Physical Security)

It is important to ensure that your computer equipment is physically secure so that criminals cannot steal and access data. Computer equipment is also vulnerable to fire, flood and accidental damage. The consequences can be devastating if you lose data due to one of these reasons.

Keep your Computers Safe:

- Keep doors and windows locked
- Fit an intruder alarm and CCTV
- Consider proprietary computer locking plates or secure computer enclosures for high value items
- Take care how you dispose of packaging that might advertise that you have new equipment
- Consult with your insurance company and local Crime Prevention Officer for additional security advice

IT Infrastructure:

- Keep servers and network equipment in a locked room and control access to it
- Server and networking racks and cabinets can also be protected by individual locks
- Locate equipment to minimise risks from fire, flooding and theft
- Keep a fire extinguisher, suitable for use with electrical equipment, close to the important IT equipment
- Consider active fire suppression systems (gas, sprinklers, water mist etc.) for critical installations, along with rapid response aspirating smoke detection systems

Hard Copy Records:

- Use lockable filing cabinets
- Maintain a strict shredding policy
- Have a “clear desk” policy so that employees lock up sensitive papers when they are not working on them

Limit the impact of a Theft or Loss:

- Make a note of all IT equipment serial numbers to enable reporting if stolen
- Security mark computers and other high value items
- Ensure computer equipment is adequately insured
- Back up data and ensure copies are kept off site at all times
- Have an effective Business Continuity Plan (BCP) that is regularly tested

Visitors

- Be vigilant about granting access to any visitors and escort them where appropriate
- Vet contractors and support personnel
- Restrict access to sensitive areas

By recognising these three security aspects (Data, Network and Physical) you can considerably enhance your ability to control Data Security.

Insurance Solution for Data Risks

A targeted attack on your system or the loss of a laptop containing sensitive data could expose your business to a range of costs and expenses.

There are a range of insurance solutions available that can provide cover for:

Breach costs

- Forensic investigations: costs to find out what went wrong and to confirm whose data has been put at risk
- Notification: whether to individuals, the payment card industry (PCI) or a regulator, cover for your costs to draft and deliver notifications
- Cover for: costs if you need to set up a call centre or offer credit monitoring services to affected customers.
- Public relations: if you need support in rebuilding your reputation, Insurers can cover the costs to employ a specialist firm

Privacy protection

- Third party liability: defend and settle claims against you for failing to keep your personal data secure
- Regulatory actions: investigations by regulators or the PCI can be expensive to defend. Insurers will pay for defence costs and have no hourly rate cap for legal services. Cover also for civil penalties (where allowed) and compensatory awards levied by regulators.

Cyber business interruption

How would you be affected if a hacker, competitor or other third-party targeted your computer systems to prevent you earning revenue online? Insurers' cyber business interruption module aims to compensate you for earnings you miss out on in this situation.

Cyber liability

The content of a website or an email to a client can easily be read the wrong way, or could have mistakenly infringed someone's copyright. Under the Insurers' Cyber Liability module, we will work with you to respond to claims which arise out of your online content

Hacker damage

If a hacker causes damage to your websites, programs or electronic data, or steals any program or data you hold electronically, Insurers' hacker damage module will reimburse you for costs of repair, replacement or restoration

Cyber extortion

Rather than hack into and damage your websites or data, a hacker may hold your business to ransom at the threat of doing so. As well as instructing a leading security risk consultancy firm to assist in the handling of the situation, Insurers' cyber extortion module would cover you for any final ransom paid to minimise the disruption to your operations

Info courtesy of **RiskSTOP Group Limited**
More information can be found on their website: www.riskstop.co.uk