WHAT YOU SHOULD KNOW ABOUT DATA PROTECTION

An Information Security Management System for SMEs
Foreward

“The blunt truth is that all organisations need to take the protection of customer data with the utmost seriousness. I have made clear publicly on several occasions over the past year that organisations holding individuals’ data must in particular take steps to ensure that it is adequately protected from loss or theft. There have been several high-profile incidents of data loss in public and private sectors during that time which have highlighted that some organisations could do much better. The coverage of these incidents has also raised public awareness of how lost or stolen data can be used for crimes like identity fraud. Getting data protection wrong can bring commercial, reputational, regulatory and legal penalties. Getting it right brings rewards in terms of customer trust and confidence”.

Tony Richardson  CISSP

Tony.richardson@octree.co.uk

www.octree.co.uk

www.securapro.co.uk

T:  08456 171819
M: 07967 033487

Octree Limited
The Iloyds Building
Birds Hill
Letchworth
Herts.  SG6 1JE
Legal and Regulatory Obligations

- The Data Protection 1998
- PCI-DSS v2
- Computer Misuse Act 1990
- The ICO can issue fines up to £500,000
Data Protection

Principles of the Data Protection Act 1998

The seventh principle:

- should be subject to appropriate technical and organisational measures to prevent the unauthorised or unlawful processing of personal data, or the accidental loss, destruction, or damage to personal data;
The Solution – a 15 point plan

• 1 Risk Assessment

  ▪ Identify all your information assets
  
  ▪ Assess the potential threats to those assets – environmental, natural, human
  
  ▪ Determine the possible vulnerabilities in those assets
  
  ▪ Consider, and deploy, the necessary countermeasures
  
  ▪ Review
The Solution – a 15 point plan

• 2 Governance

- Develop a security policy document that everyone, from senior management to junior members of staff can “buy in to”.

- Develop specific policies to address:
  - Passwords
  - USB devices
  - Remote Access
  - Acceptable use of computer resources
The Solution – a 15 point plan

- **3 Training and Awareness**
  
  - Make everybody aware of the risks
    
    - Innovative training programmes
    - Wall posters
    - Screensavers
    - Newsletters
    - Security intranet portal
The Solution – a 15 point plan

- 4 Servers, Desktops and laptops

- If customer data is stored on a Laptop, Desktop, or a File Server you need to have the following security precautions in place:
  - Properly configured Firewall
  - Antivirus and Antispyware Software
  - Full Disk Encryption
  - Removable Device Encryption
The Solution – a 15 point plan

5 Password protection

Password protection of all computers is essential!!!

- At least 8 characters long, containing letters, numbers, capitals and other symbols i.e. P@nD4b34R!
- Easy to remember but hard to guess
- Avoid any word in the dictionary, personal information such as a child or partner’s name or a football team, common names and slang.
- Try playing on normal words such as England – 3nG1@Nd!
- Do not write passwords down
- Do not tell anyone else your passwords
- Change your password every 90 days at the very least!
The Solution – a 15 point plan

- **6 Email security**

- All emails containing customer data must be secure.

- Avoid spam and email borne viruses and malware

Police your email usage policy to avoid data leakage and litigation.
The Solution – a 15 point plan

• 7 Physical Security

  • Physical security is a key factor in securing your data.
  
  • Your servers, and external storage devices containing confidential data, should all be kept in a locked cabinet within a secure room to prevent casual access.
  
  • Environmental considerations such as battery backup, fire prevention, and air-conditioning need to be made.
  
  • Know and control who has access to your offices and when.
The Solution – a 15 point plan

- **8 Backups**

  - Full backups of all critical data should be standard practice:
    - Backup media should be locked away securely while not in use.
    - Only authorized personnel should have access to backup media.
    - Backup media should be held off site for disaster recovery.
    - If the media is held off site it should be transported and stored securely i.e. a lock box or safe.
    - Back up media needs to be encrypted.
The Solution – a 15 point plan

- **9 Access Control**
  - Users should only have permission to access to confidential information they need to do their job.
  - You should review access permissions for every user at regular intervals.
  - Each employee should have their own logon account.
  - Employee’s access should be revoked as soon as they leave the company or are suspended.
  - Locations where sensitive or confidential information is stored should be audited.
The Solution – a 15 point plan

10 Data Transfer

Any movement of data outside of your secure environment, e.g. USB or CD, needs to follow these guidelines:

- Encrypt all portable media using a suitable encryption technique.
- Use device control software to control and detect unauthorized access to external media such as CDs and USB devices.
- Keep a record of all of these devices and which personnel are allowed to use them and for which purpose.
The Solution – a 15 point plan

• 11 Asset management

- keep a record of all computers, laptops, USB devices, external hard drives, printers, network devices, wireless devices, etc. that exist in your business.

- maintain a record of all data copied onto media moving outside your secure environment, and the reason for doing so.
The Solution – a 15 point plan

- **12 Data destruction**

Data removal and destruction is an important part of keeping your clients’ information secure.

- Paper records need to be shredded in house or by an approved agency that must be vetted.

- Hard drives should be disposed of securely ensuring all data is destroyed.

- Certificates should be obtained from agencies confirming destruction of data from hard drives and recycled computer systems.
The Solution – a 15 point plan

13 Remote access

- Remote access to your network needs to be secure.

- Remote access and VPN software needs to be configured properly for the highest possible security level.

- Home workers need to ensure that any wireless network is encrypted to the highest possible standards.

- Home workers need to prevent unauthorised access to their computer systems through password protection at least.
14 Staff recruitment

Where legally possible carry out every background check on staff who will be exposed to confidential information:

- credit references
- CRB checks
- CIFAS staff fraud database.
- References
- CV validation
- Assess regularly if staff in higher-risk positions may be susceptible to coercion.
The Solution – a 15 point plan

• **15 Internet access**
  
  • Implement monitoring controls for email and internet activity to identify potential data leakage and defamatory / illegal content.
  
  • Implement filtering to protect against web borne malware and viruses.
  
  • Filter access to content that allows web based communication such as webmail (Hotmail, Gmail, Yahoo, MSN instant messaging), social networking sites like Facebook and Myspace
  
  • Restrict or block access to file sharing sites.
The business risks and penalties

- Data Loss damages corporate reputation
- Data loss results in major financial loss
- Data loss compromises competitive advantage
- Data loss can affect compliance
- Data loss or non-compliance can result in fines or closure