

# **Information Security**

---

# **What is Information Security?**

**“Information is an asset which, like other important business assets, has value to an organisation and consequently needs to be suitably protected.”**

Ref: ISO/IEC 17799:2005

# What is Information Security?



---

# **What is Information Security?**

- **Confidentiality**
  - (keeping sensitive information safe)
- **Integrity**
  - (keeping information correct)
- **Availability**
  - (keeping information available)

---

## **Why is Information Security important?**

- **Compliance with Law Society Guidelines**
- **Reputation**
- **Continuity**
- **New business**

---

## **Common Myths About Information Security**

- Myth 1: Information Security is the concern and responsibility of the IT Director
- Myth 2: Security Threats from outsiders are the greatest source of risks
- Myth 3: Information Security is assured by safeguarding networks and the IT infrastructure
- Myth 4: Managing People issues is not as important
- Myth 5: Adopting latest technological solutions will increase security

---

# **Cases where IS has been compromised**

## **Confidentiality**

- Sir Philip Green (BHS) take over of M&S
- Use of Freshfields, M&S Legal advisors, Barry O'Brien
- Injunction and fine of £9K and had to pay agreed costs of £50K

---

# Cases where IS has been compromised

## Integrity



- **John Profumo affair in 1961**

# Cases where IS has been compromised

## Availability



- **Victims of “Benji the Binman” have been:  
Sir Elton John, Mohamad Al Fyed, Robbie Williams,  
All Saints, and Sir Richard Branson**

## Why Bond Pearce Chose to Certify

- Many factors influenced the decision
- More and more tenders were asking IS related questions
- Draft Law Society / SRA Guidelines eluded to ISO 27001

## Why bother with security?

- Compromised company information can benefit our competitors and inhibit our success.
- Hackers and viruses can destroy your work.
- Your private information can be compromised.
- Your ability to work can be hampered.

---

# **Building Information Security**

- **Know the Asset**
- **Know the Asset's value**
- **Know the risks (and how to reduce)**

---

## Desired Goals

**Confidentiality** (keep it secret)

**Integrity** (keep it accurate)

**Availability** (keep it available)

---

## **Various information states**

- **Whilst it is being transmitted**
- **Whilst it is being stored**
- **Whilst it is being processed**

---

# Safeguards

- **Human factors**
- **Policy and Process** (Security culture)
- **Technology**

---

## **How did Bond Pearce Achieve ISO 27001**

- Took 18+ months to be ready for certification
- Effort involved for certification rather than compliance was minimal
- Nothing was left out of scope

---

# **How BP built a security culture**

- **High level policy**
- **Champion**
- **Functional policies**
- **The responsible person**
- **Enable the business (don't stop it)**
- **Awareness**
- **Learn from experience**

---

## **Obstacles Experienced**

- Change culture – no one likes change
- Raising general awareness
- Ensuring policies were correct and enabling

## Some Information Security Basic Principles

- Wear your security badge at all times.
- Do not attempt to install any software unless explicitly authorised by the IT department.
- Use WinKey + L to lock your screen if you are away from your desk.
- Do not tell anyone else your password(s), or write them down.
- Do not log anyone else into the system using your login ID.
- Do not open any suspicious emails.
- Report any suspected infection to the IT Service Desk immediately!
- Ensure confidential documentation is locked away when not in use.
- Be vigilant and report anyone you do not recognise to Office Manager.
- Security is everyone's responsibility.

# What should be kept secure?

## Obvious examples

- Finance department data
- Research and development data
- Human resources personnel files
- Any business information marked *Confidential*
- Client information

## Less obvious examples

- A Partner's contact list
- A Partner's e-mail messages
- Direct telephone numbers
- Personal employee telephone numbers

# IT Responsibilities

- Log all Information Security incidents
- Write or re-write Policies as appropriate to business needs
- Enforce policies where appropriate
- Ensure regular review of permissions and access
- Ensure ISMS is kept up to date
- Give Information Security Awareness sessions as appropriate
- Ensure the BCP & DRP are tested annually
- Maintain internet and email controls as agreed and monitor (where needed) on a regular basis
- Liaise with third party security organisations on threats etc...
- Ensure all applications fit the Information Security model and are risk assessed before implementation

---

## • HR Responsibilities

- Aid with enforcement of Policies as needed
- Ensure recruitment checks are performed accurately
- Ensure personnel details are accurate
- Ensure leaver processes are adhered to, ensuring line managers are aware of and understand their responsibilities

---

## • Facilities Responsibilities

- Ensure building security is maintained at all times
- Ensure door access (where appropriate) is reviewed on a regular basis
- Ensure adequate storage is available if required
- Ensure compliance with Fire Regulations and conduct regular fire evacuation tests/drills

---

## A Few Facts...

- More than 70% of people would reveal their computer password in exchange for a bar of chocolate and through social engineering
- 34% revealed they used a pet or child's name
- 33% said they shared passwords or wrote them down
- People do not like confronting strangers.
- Tail gating is the most common form of access

Ref: BBC News <http://news.bbc.co.uk/1/hi/technology/3639679.stm>

## Timescales

Task	Apr, 07	Jul, 07	Nov, 07	Dec, 07	Jan, 08	Mar, 08	May, 08	Jun, 08	Jul, 08	Sep, 08
GAP Analysis										
Project Approval										
Documentation										
Check										
Training										
Assessment										

# Questions?

