
 **LOCKTON**

 **Computer Law Training**  
Data matters

WELCOME TO LOCKTON'S WEBINAR:  
*Information Security Risks*

April 2014

**Tim Musson**  
**Computer Law Training Ltd**

**Calum MacLean**  
**Lockton Companies LLP**

## Overview

- ❑ Information Security risks: perception v reality
- ❑ Vulnerabilities & threats – prioritised
- ❑ Recent Examples
- ❑ Practical steps to protect yourself and your firm

## Information Security – the reality

Computer Law Training

Data matters

■ **25%**

Organisations admit to security breaches in the last year

■ **36%**

expect a security breach in next 12 months

■ **84%**

employees believe that colleagues violate controls on storage and use of electronic data

■ **96%**

data leaks are inadvertent

Source: Titus.com

LOCKTON

2

## Information Security Trends

Computer Law Training

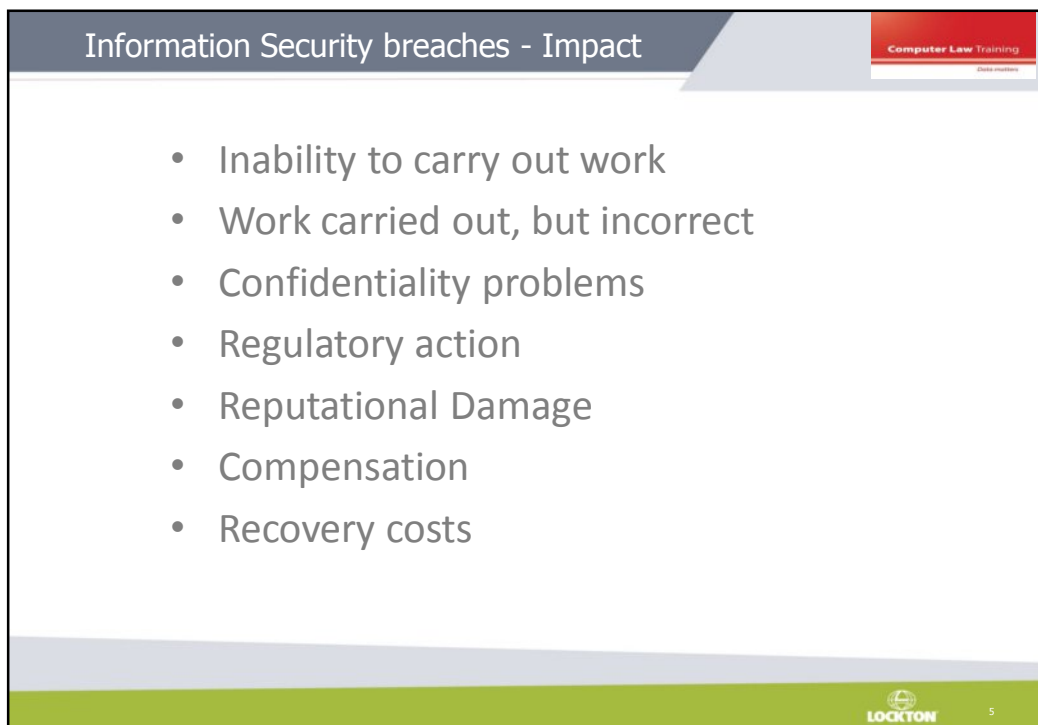
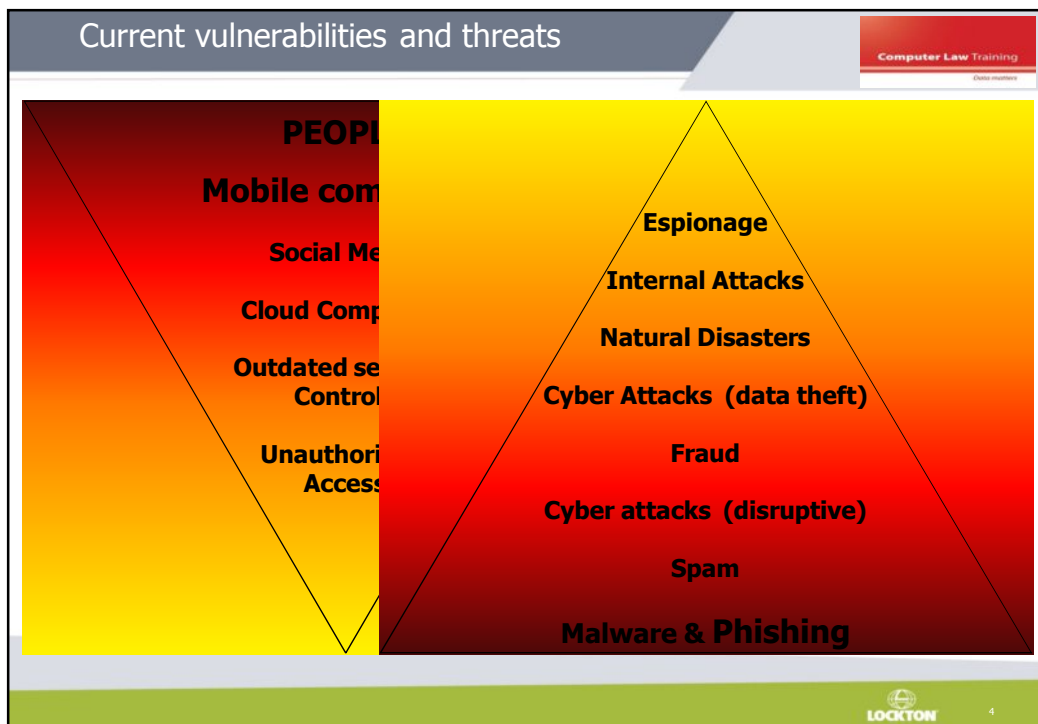
Data matters

**FUTURE TECHNOLOGIES**

- ☐ Digital Money
- ☐ In-memory computing
- ☐ Cyber havens
- ☐ Internet of things

LOCKTON

3



Case-study 1: The **Epsilon** Data Breach

Computer Law Training

**Important information from M&S**



[Add to contacts](#)  
 To

We have been informed by Epsilon, a company we use to send emails to our customers, that some M&S customer email addresses have been accessed without authorisation.

We would like to reassure you that the only information that may have been accessed is your name and email address. **No other personal information, such as your account details, has been accessed or is at risk.**

We wanted to bring this to your attention as it is possible that you may receive spam email messages as a result. We apologise for any inconvenience this may cause you. We take your privacy very seriously, and we will continue to work diligently to protect your personal information.


Marks and Spencer plc. Registered office: Wiltshire House, 35 North Wharf Road, London W2 1NW.  
 Registered number: 214436 (England and Wales)

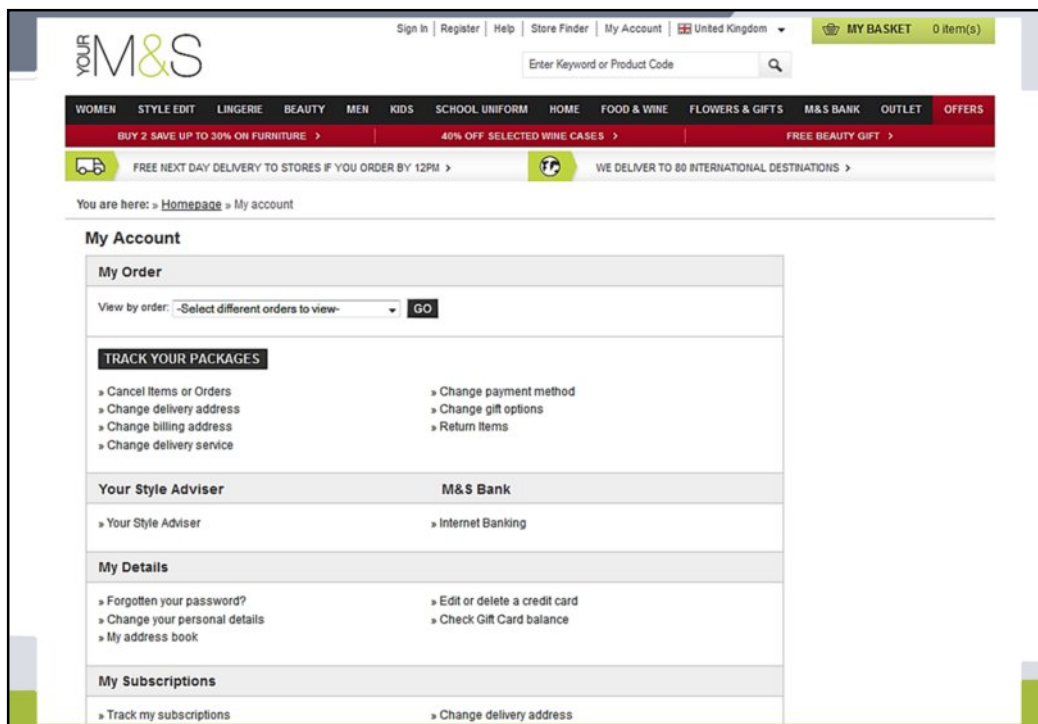

6

Case-study 1: The **Epsilon** Data Breach

Computer Law Training

- **Cause:** spear phishing attack, downloaded
  - Win32.BlkIC.IMG - an antivirus disabler
  - iStealer - a keylogger
  - CyberGate - a remote administration tool
- **Primary Victim:** 50+ corporate clients' data
- **Secondary Victim:** 60 million people including clients of JP Morgan Chase; Capital One, Visa, M&S, Citibank
- **Impact:** *Only* names & email addresses?

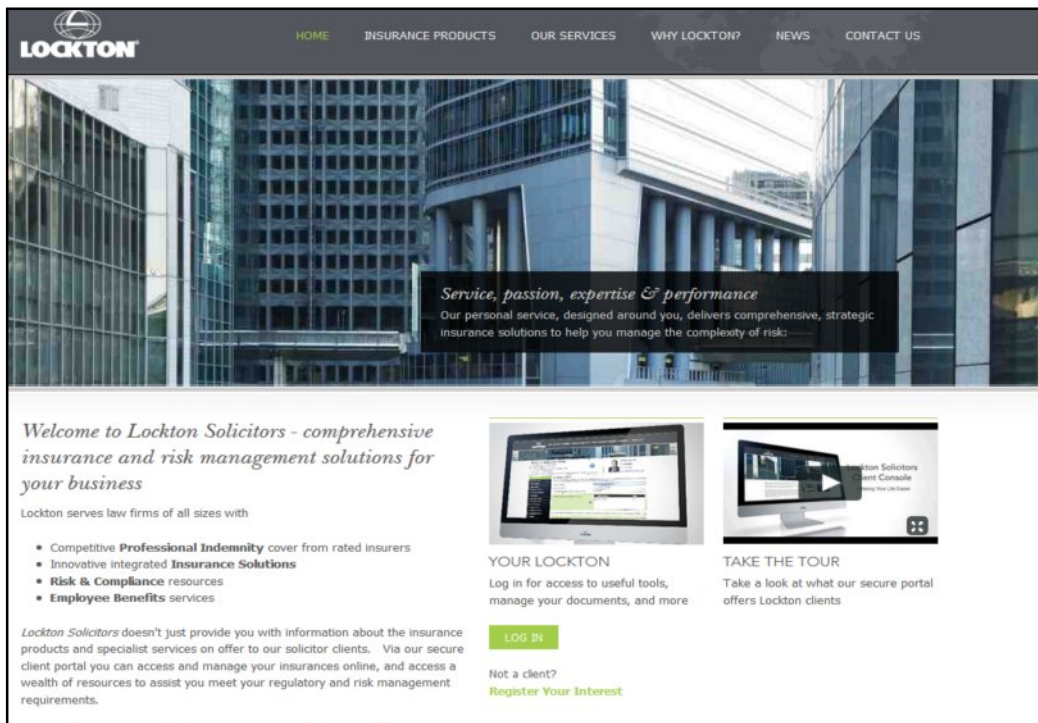
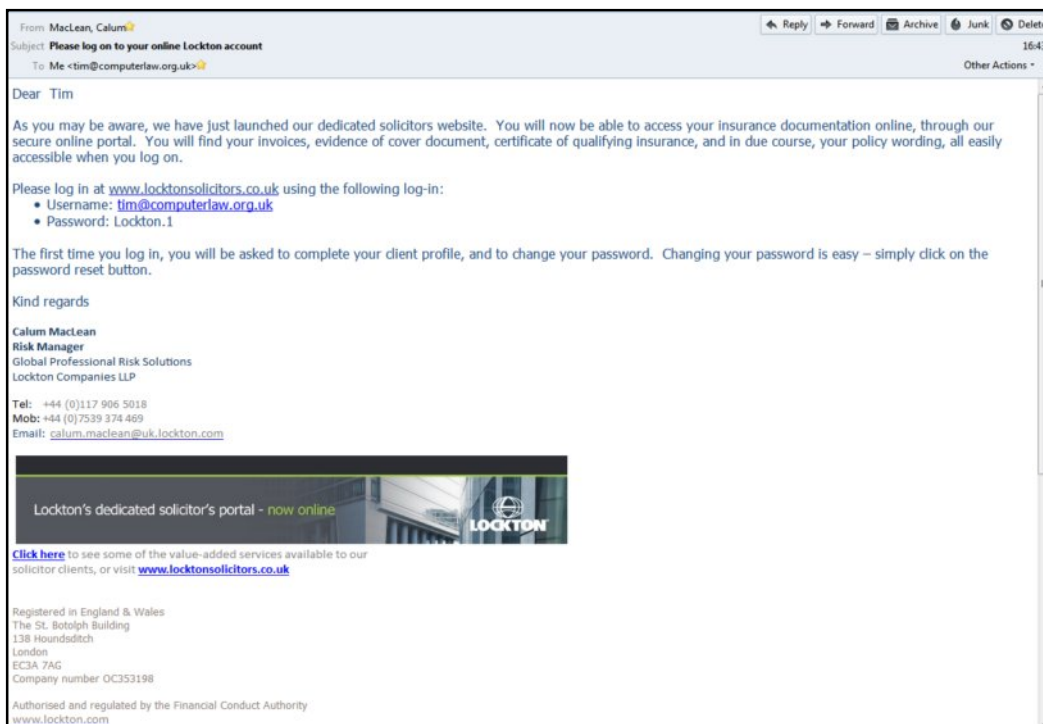

7



## Case-study 2: A Spear-Phishing Attack

Computer Law Training

- Target: Lockton clients
- Source of email addresses:
  - hack Lockton system for access to database, or identify compliance officers in law, accounting and IFA firms and rely on statistics
- URL: [locktonsolicitors.co.uk](http://locktonsolicitors.co.uk) and [lockton.com](http://lockton.com) are available
- Create email account: [calum.macLean@uk.lockton.com](mailto:calum.macLean@uk.lockton.com)
- Cloned website [www.locktonsolicitors.co.uk](http://www.locktonsolicitors.co.uk)
- Send emails
- Wait for keyloggers to be installed

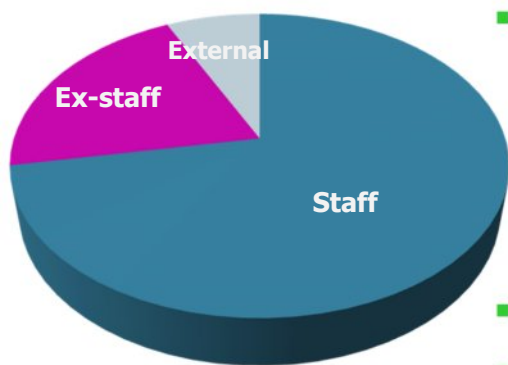


## Heartbleed

- Heartbleed allows a hacker to collect sensitive information, including logins and passwords from vulnerable websites (c. two thirds of websites).
- Check vulnerability of a website at [lastpass.com/heartbleed](http://lastpass.com/heartbleed)
- If vulnerable change your password!



## Threats: Who is a Threat?



- **Carelessness, stupidity, malice?**
  - Emails
  - Careless conversations
  - Remote working
  - BYOD
- Shared passwords
- Social media



## Internal Threats: Risk Controls

Computer Law Training

Data security

## ■ Awareness campaigns

## Awareness Campaigns – resources from Lockton

**Follow a CLE desk**

1. Lock / turn off
2. Put confidential
3. Don't leave any
4. Don't leave your
5. Ensure document
6. Lock your desk

**Who's LISTENING?**

Be aware of who may be listening, when sharing confidential information on IT

**How do YOU**

Encrypt anything you need to keep  
Secure your memory stick - store it!  
Keep another copy of all files...

- 17,000+ lost annually in the UK
- Can store over 80,000 pages!
- Potential for up to a £300,000

**How safe IS YOUR smartphone?**

- Is it encrypted and password protected?
- Is it protected with up-to-date antivirus software?
- What apps have you downloaded? Did you know that many carry malware and spyware?
- Do you access work emails and documents with yours?
- Do you use public Wi-Fi?

**Know the risks. Protect yourself and your clients.**

**LOCKTON**



## Internal Threats: Risk Controls

Computer Law Training

Data module

- Awareness campaigns
- Logging & reporting of breaches/near misses
- Work systems, procedures and policies
- IT systems reports & logs
- Restrictions
- Whistleblowing
- Supervision
- Leavers procedures & checklist

## External Threats

Computer Law Training

Data module

- **Technical threats**
  - Hacking
  - Malware
  - Denial of Service
- **Physical**
  - Access controls
  - Space planning
- **Social engineering**

## External Threats: Risk Controls

Computer Law Training

- Network Security Devices
- Security Management monitoring systems
- Email & data download traffic monitoring
- Physical office security
- Clear desk policy
- Effective controls on portable devices
- Vetting of suppliers (see Lockton guidance on Cloud Providers)
- Staff awareness training



18

## External Threats: Risk Controls

Computer Law Training

- Staff awareness training must emphasise Social Engineering:
  - The psychological manipulation of people into performing actions or divulging confidential information
  - Includes phishing, baiting and pretexting (or blagging)



19

## External Threats: Testing

Computer Law Training

- Effectiveness of external threat controls should be checked using Penetration Testing (Pen Testing)
- An external contractor tries to penetrate the system, to either install malware or extract information, using both technical hacking and social engineering
- Results of pen testing used in staff training



20

## External & Internal Threats: Encryption

Computer Law Training

- If information which falls into the wrong hands is encrypted then the problem is minimised
- Candidates for encryption include:
  - Portable devices (laptops, memory sticks, smartphones, etc)
  - Emails
  - Cloud backups



21

## Governance

Computer Law Training

Data matters

- If information security is to be taken seriously in an organisation it needs to be the responsibility of an individual or committee at the top level of an organisation
- There needs to be clear procedures, lines of authority, enforcement and monitoring mechanisms and technologies that ensure the security of an organisation's electronic assets
- Aims:
  - Strategic alignment of information security with business strategy
  - Risk management
  - Resource management
  - Performance measurement
  - Value delivery



22

## Top Ten Action Points

Computer Law Training

Data matters

1. Ensure that there is an information security champion at top level of the organisation
  - Ask for a volunteer at board level. Alternatively appoint someone to take responsibility. Preferably not someone with IT responsibility. Ideally should also have either business development or operational responsibilities.
2. Encourage reporting of data breaches and near misses
  - Everyone makes mistakes, including senior management. They should set an example of reporting and this should be accessible for staff.
  - Keep a breaches register, monitor it regularly, take action



23

## Top Ten Action Points

Computer Law Training

3. Discourage a blame culture
  - As above!
4. Implement staff (including senior management) training on a regular basis
  - Senior management must attend training to show importance of security. Training should include motivation and behavioural issues. Use a reputable provider!
5. Create clear acceptable use, security, mobile device and social media policies and make them easily accessible
  - Guidance on security related policies can be found at [www.sans.org/security-resources/policies/](http://www.sans.org/security-resources/policies/)

## Top Ten Action Points

Computer Law Training

6. Use encryption for sensitive data wherever possible
  - IT staff (internal or external) should be able to deal with technical aspects of this.
7. Enforce good password management
  - Useful guidance can be found at [en.wikipedia.org/wiki/Password\\_policy](http://en.wikipedia.org/wiki/Password_policy).
  - IT staff should be able to enforce technical aspects.
8. Ensure that security enables business and does not prevent it – there will always be some security risk
  - Risk should be minimised while allowing necessary activities to be carried out

## Top Ten Action Points

Computer Law Training

Data security

### 9. Do not allow staff to download and install software from the internet

- IT staff can enforce this. Find out why software is wanted, decide if need is valid and obtain clean software if necessary.

### 10. Back-up all important files onsite and offsite

- Offsite back-ups may be cloud based or in another branch of the firm. Check regularly that back-ups can be read.



26

#### Our Mission

To be the worldwide value and service leader in insurance brokerage and risk management

#### Our Goal

To be the best place to do business and to work



Lockton Companies LLP

Authorised and regulated by the Financial Conduct Authority.

A Lloyd's broker Registered in England & Wales at: The St Botolph Building, 138 Houndsditch, London, EC3A 7AG.

Company No. OC353198

[www.lockton.com](http://www.lockton.com)