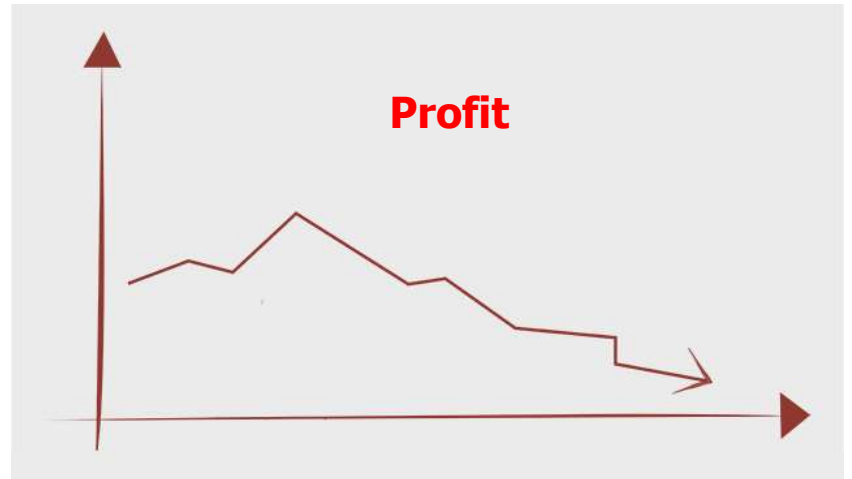




# Information Security & Fraud Risks: A practical guide

Presented by  
**Calum MacLean**  
Risk Manager,  
Lockton Companies LLP

# Information Security & Fraud: The real implications for professional firms



## What is at risk?



# Vulnerabilities & Threats

People  
Mobile computing  
Social Media  
Cloud Computing  
Outdated security  
Controls  
Unauthorised  
Access

Espionage  
Internal  
Attacks  
Natural Disasters  
Cyber Attacks  
(data theft)  
Fraud  
Cyber attacks  
(disruptive)  
Spam  
Malware & Phishing

# Threats & Financial Impact

**Human error**



**IT system failure**



**Third-party IT security failure**



**Cyber security or data breach**



**Data loss from backup/restore failure**



**Natural or manmade disaster**



Source: IBM/Ponemon Institute Global Study of the Economic Impact of IT Risk, 2013

**Cyber crime costs small-medium UK businesses £800m a year**

**18m new malware types released in Q2 of 2013 alone (McAfee 2013)**

---

## Information Security: What is it?

**25%** Organisations admit to security breaches in the last year

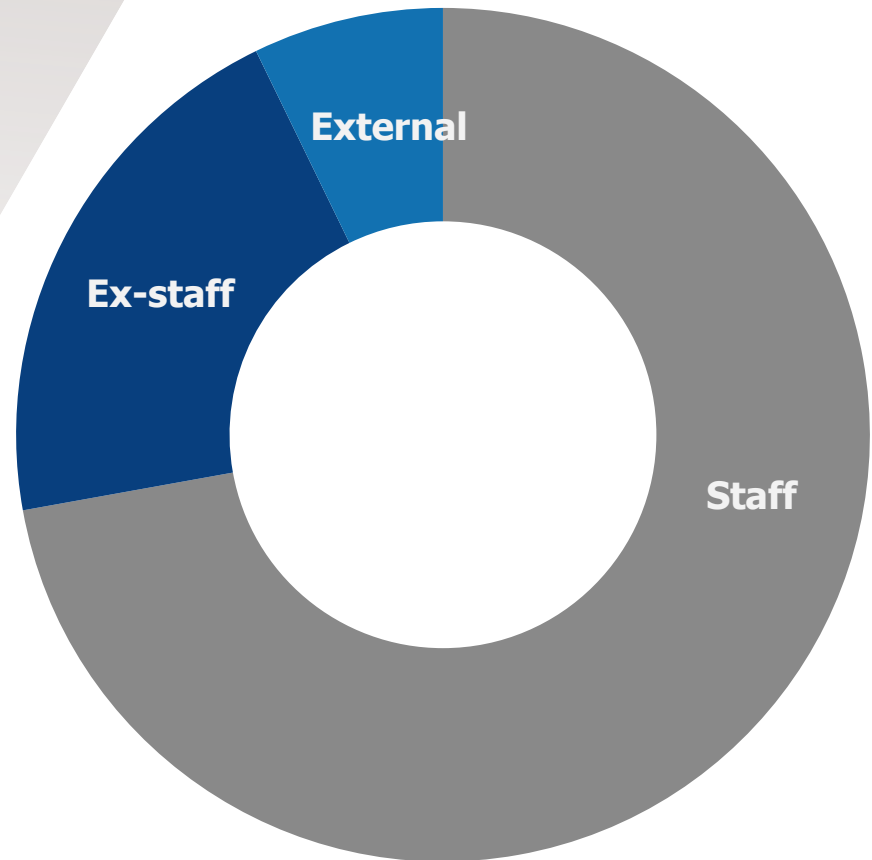
**36%** expect a security breach in next 12 months

**84%** employees believe that colleagues violate controls on storage and use of electronic data

**96%** data leaks are inadvertant

# People Risks

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



# People Risks: Mitigations



**Recruitment:  
references &  
vetting**

**Regular,  
Practically-focussed,  
refresher training**



**Supervision**

**Systems &  
Procedures**





# Awareness Campaigns

Follow a **CLEAR** desk policy.

1. Lock / turn off your computer.
2. Put confidential papers away.
3. Don't leave smartphones or other portable devices unlocked/unattended on your desk for any length of time.
4. Don't leave your security pass or keys unattended.
5. Ensure documents containing sensitive information are disposed of securely
6. Lock your desk drawers and cabinets before leaving for the day.



Lockton Companies LLP. Authorized and regulated by the Financial Conduct Authority. A Lloyd's broker Registered in England & Wales at The 25 Bankside Building, 1SE 1JX London, EC3A 7NL. Company No. 06253396. LLP 1291. [www.lockton.com](http://www.lockton.com)



How do **YOU USE** yours?

Encrypt anything you need to keep private. Secure your memory stick - close it safely. Keep a further copy of all files.

- 17,000+ lost annually in the UK (Credit Technologies, 2011).
- Can store over 80,000 pages confidential data (4GB USB).
- Potential for up to a £100,000 claim.



Lockton Companies LLP. Authorized and regulated by the Financial Conduct Authority. A Lloyd's broker Registered in England & Wales at The 25 Bankside Building, 1SE 1JX London, EC3A 7NL. Company No. 06253396. LLP 1291. [www.lockton.com](http://www.lockton.com)



Who's **LISTENING** in?

Be aware of who may be listening, when sharing confidential information on the phone.



Lockton Companies LLP. Authorized and regulated by the Financial Conduct Authority. A Lloyd's broker Registered in England & Wales at The 25 Bankside Building, 1SE 1JX London, EC3A 7NL. Company No. 06253396. LLP 1291. [www.lockton.com](http://www.lockton.com)



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 Companies LLP. Authorized and regulated by the Financial Conduct Authority. A Lloyd's broker Registered in England & Wales at The 25 Bankside Building, 1SE 1JX London, EC3A 7NL. Company No. 06253396. LLP 1291. [www.lockton.com](http://www.lockton.com)



---

## Frauds & Scams

Identity fraud

Social Engineering

Fake Law firms

Phishing

Trojans

Vishing

Invoice Hijacking



---

# Targetting Identity Fraud

- Client & Transaction Vetting
- AML Processes
- Identification of Documents
- Training



# Transaction/Client Vetting

## TRANSACTION VETTING: ANTI MONEY LAUNDERING RISK ASSESSMENT

If you do not already have a system for evaluating AML risks as part of your transaction vetting procedures, this simple risk assessment matrix may provide a useful starting point. If a transaction is scoring a significant number of amber/red responses, consider escalating your ID checks and other vetting procedures – in addition to referring to your firm’s MLRO.

Risk	Score ratings descriptions			Assessments											
	Score rating = 1	Score rating = 2	Score rating = 3	Initial			Review 1			Review 2			Final		
Type of client	Individual – checked/known UK Company - known	Previously unknown UK Co. Checked/known UK Trust	Foreign Company Previously unknown UK Trust	1	2	3	1	2	3	1	2	3	1	2	3
Type of transaction	Civil Court Matrimonial Sale of House (known client) Will/Executry	Conveyancing (known purchaser) Commercial transaction Sale of House (unknown client) Confirmation (known client)	Conveyancing purchase (unknown purchaser)  Company formation (unknown client)	1	2	3	1	2	3	1	2	3	1	2	3
Introductory source	Existing client Personally introduced by well known, trusted individual (solicitor, accountant, in bank)	New client, introduced by existing client. Known firm of solicitors Recognised introductory source.	Off the street  Unknown introductory source	1	2	3	1	2	3	1	2	3	1	2	3
Value of Transaction (not necessarily fee)	Nil/small	Medium / proportionate	Large / out of proportion	1	2	3	1	2	3	1	2	3	1	2	3
Location of client	Local	UK	Elsewhere	1	2	3	1	2	3	1	2	3	1	2	3
Source of Funds	Client's own funds Solicitor's cheque From known account	Third party	Cash	1	2	3	1	2	3	1	2	3	1	2	3
Destination of Funds	Client Client's Bank Account	Third party, with justifiable reason	Third party, no demonstrable reason, non-UK	1	2	3	1	2	3	1	2	3	1	2	3
Contact	Regular face to face	Occasional face-to-face (never at their premises)	No face to face contact	1	2	3	1	2	3	1	2	3	1	2	3
				SUBTOTAL											
				RISK SCORE (total÷24)											

Notes: - ANY questions answered with a '3', or if a high proportion of '2's - refer to MLRO immediately

- ensure that all cheques, including bank drafts, are given adequate time to clear. With bank drafts, check source of funds.
- Complete final assessment prior to distributing funds.



# Social Engineering



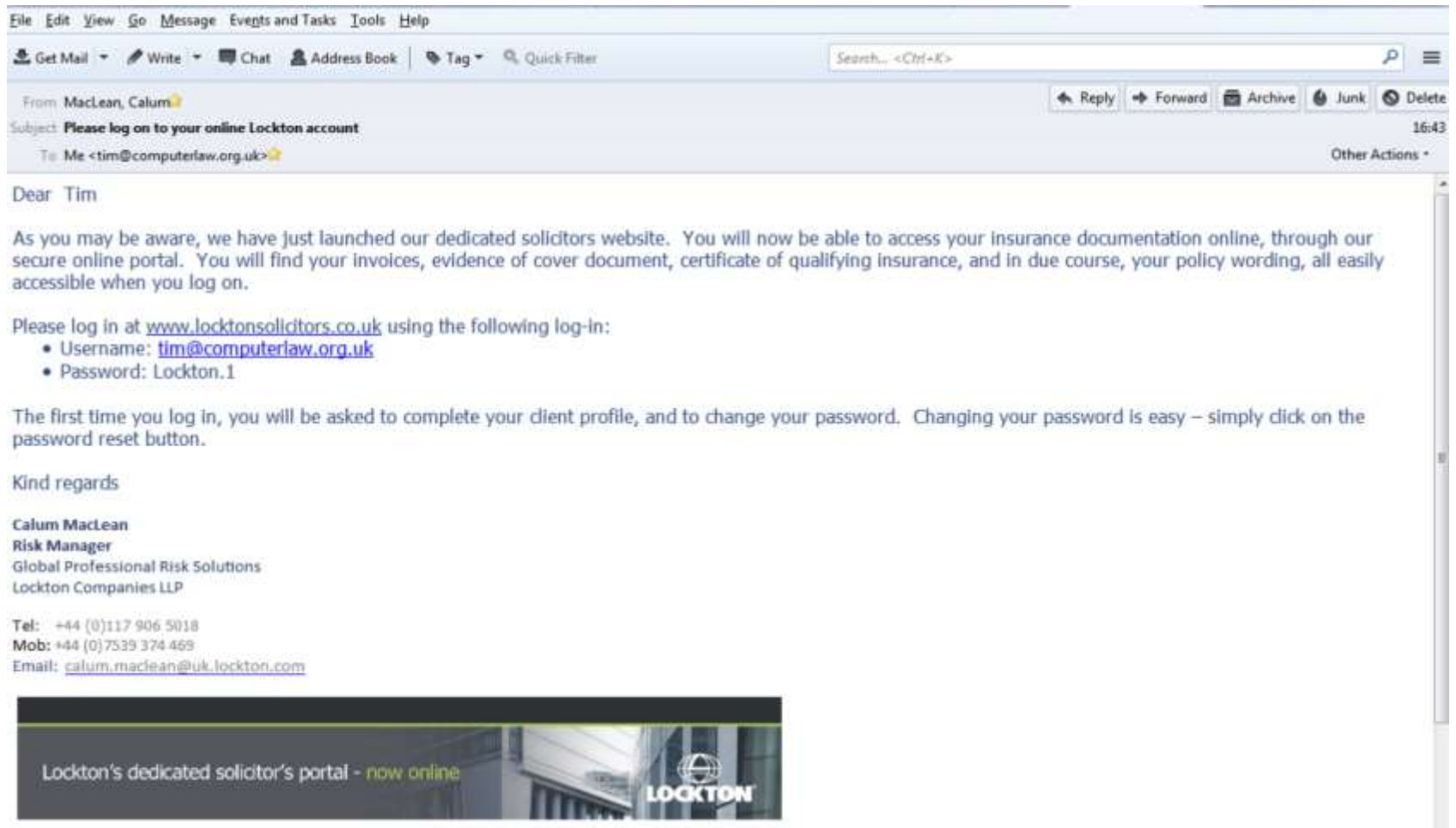
---

## Targeting Fake Law firms

1. Spelling errors and discrepancies
2. Mobile phone number only?
3. Verify the Account Number and Sort Code
4. Be wary of continued abnormal, unexplained delays
5. Continued inability to contact
6. SRA Scam Alerts (<http://www.sra.org.uk/alerts/>)
7. Alerts & Training
8. Check listings for your own firm - criminals could steal your identity too!
9. Due diligence

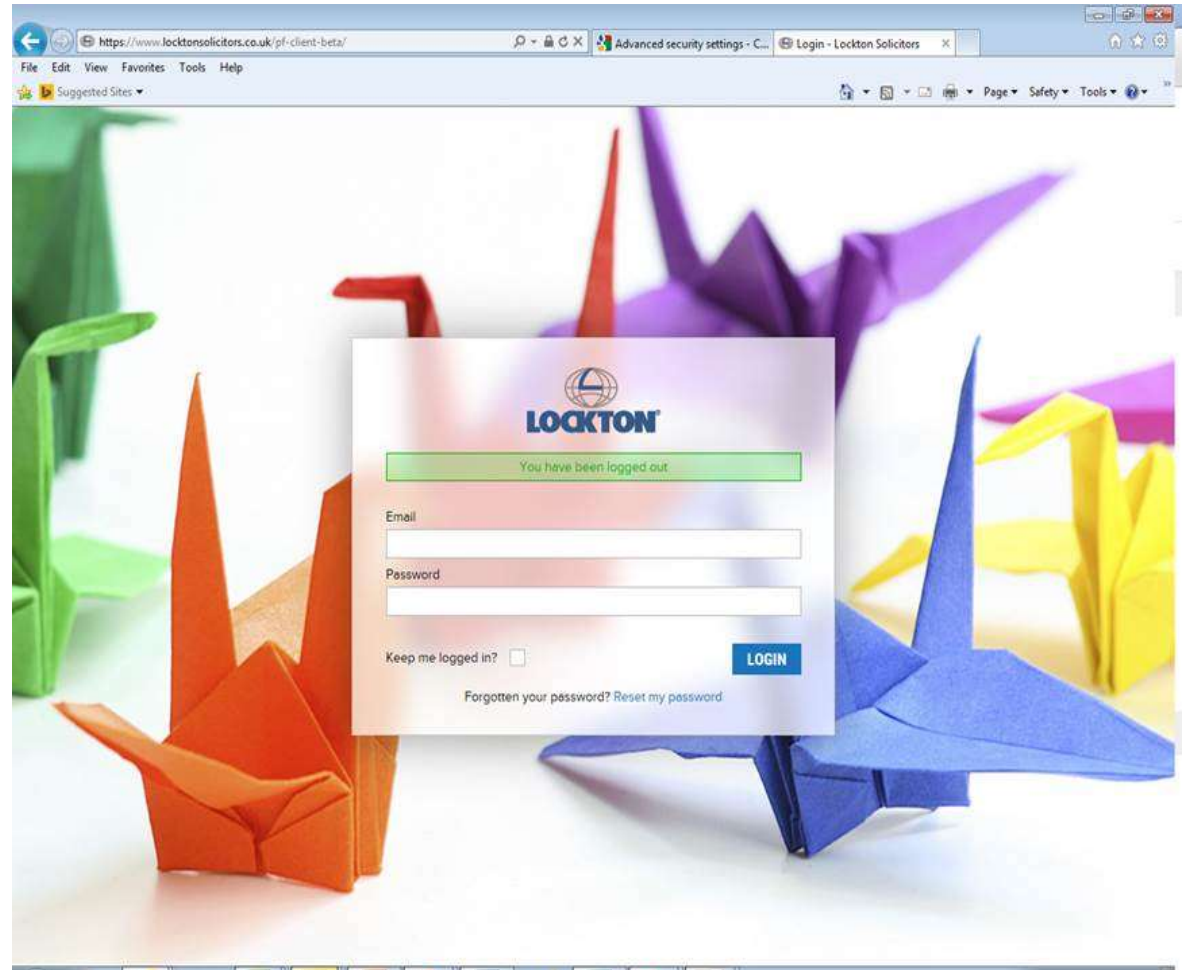


# Phishing



# Phishing

- Bogus email tricks you into visiting an apparently genuine website
- May download a trojan/spyware virus
- May ask you to provide username/password data or account details





# Vishing

- Telephone call fraud
- Impersonating bank staff
- May identify 'suspicious transactions'
- Likely to know of real genuine activity on your account also
- Will ask for detailed security information




## Vishing risk mitigation



- **HANG UP** immediately
- Use only the **OFFICIAL BANK NUMBER**
- Use a **DIFFERENT TELEPHONE**
- **EDUCATE YOUR STAFF** on the risks

# Invoice Hijacking

- Intercepting correspondence
- Usually legitimate costs
- Creation of phoney invoices with different account details



## Invoice

Account # 4301

Dealer ESI

Date 7/5/2010

Invoice # 113348

Bill To  
Law Firm

PAID

Bill To  
Law Firm

Product or Service Description	Qty	Rate	Amount
Cheques and Forms, The Bank of Nova Scotia, Trust acct. Start No.251 <i>CPA Image Ready</i> Brown/diminish DOCKET # 32200	250	0.52	130.00T
Cheques and Forms, Bank of Montreal, Trust acct. Start No. 251 <i>CPA Image Ready</i> Green/diminish DOCKET # 32083	250	0.52	130.00T
Cheques and Forms, Royal Bank of Canada, Trust acct. Start No. 1351 <i>CPA Image Ready</i> Green/diminish DOCKET # 36600	250	0.52	130.00T

VISA, MasterCard, and American Express accepted  
Please make cheques payable to ESI Software, Inc.  
Data conversion not included unless specified  
Orders with data conversions are non-refundable

---

## In Summary

- **IT:** XP, laptops, smart-phones, wifi, USB sticks
- **Systems:** access to data, restrictions
- **People:** selection, supervision, procedures
- **Information:** alerts, training, update training, reminders
- **Insurance?!**



## Questions



- As a solicitor with 8 years PQE in private practice, Calum understands risk and compliance from your perspective.
- Calum provides risk management training and consultancy to Lockton's solicitor clients, focussing on practical measures to address current and emerging risk issues . He has helped a number of clients to improve their risk profile and marketability with professional indemnity insurers.

**Email: [calum.maclean@uk.lockton.com](mailto:calum.maclean@uk.lockton.com)**



---

## Thank you for listening

CPD Hours: 1 hour  
CPD Code: EDA/LOCO

