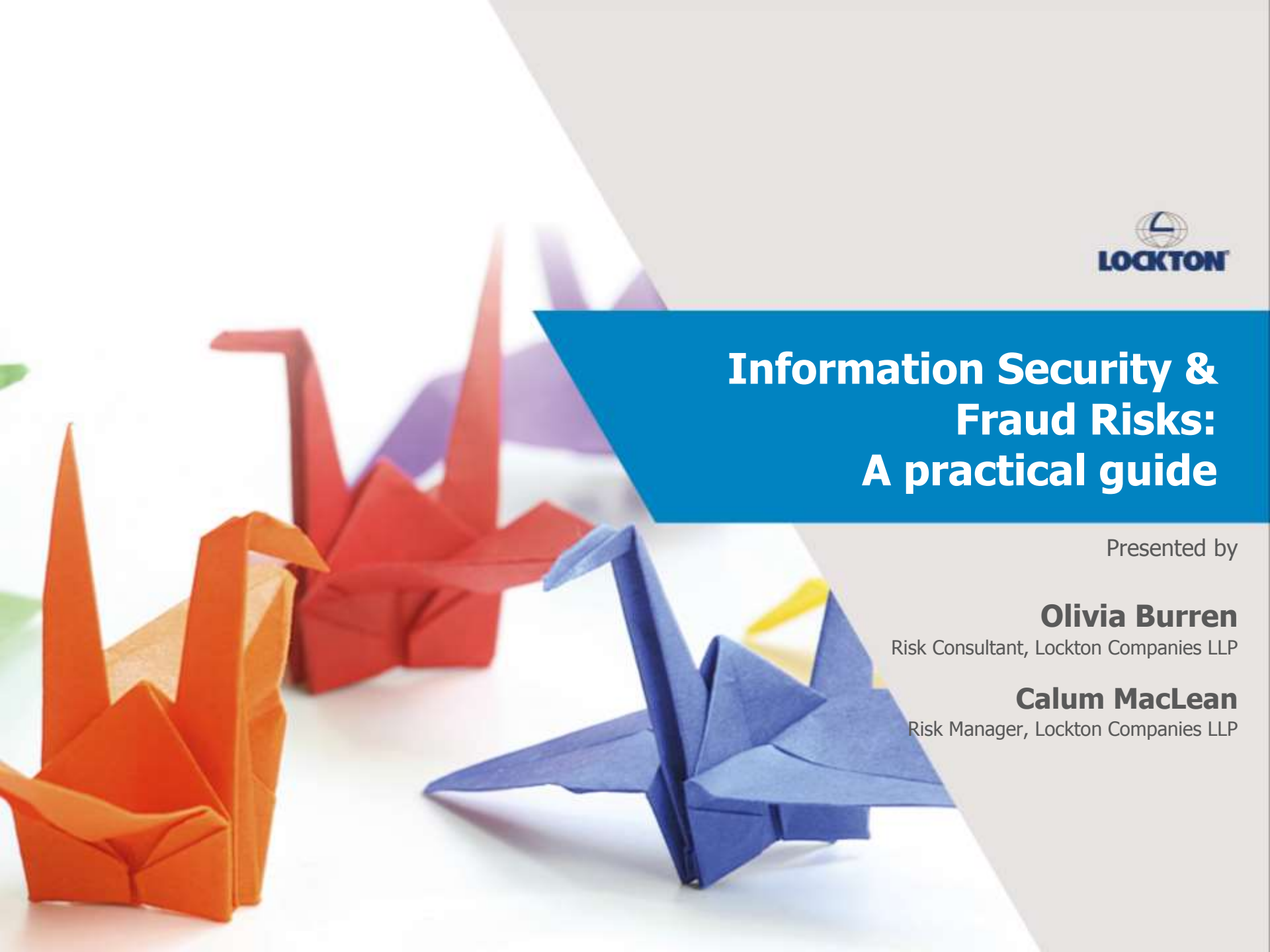


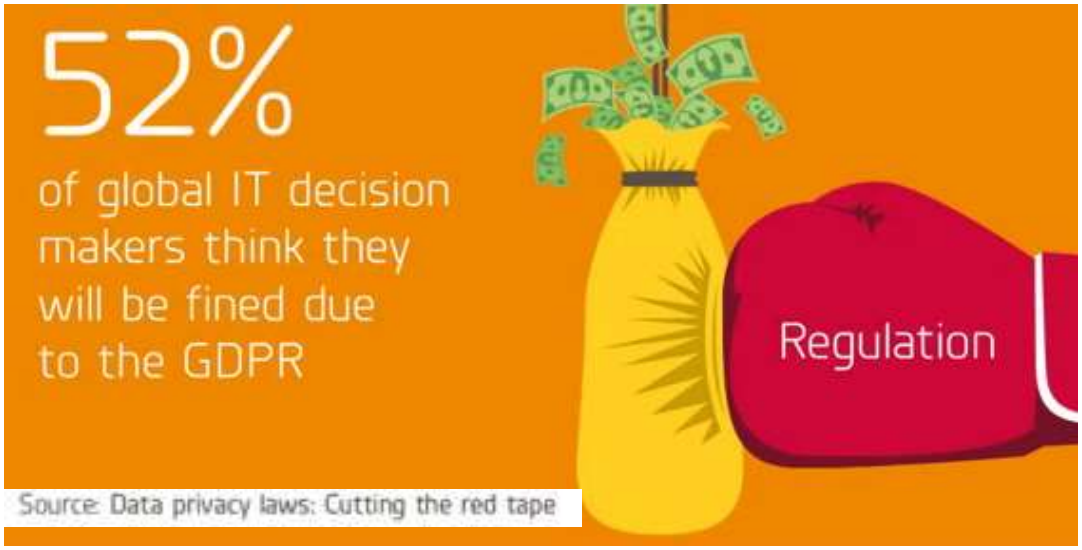
Information Security & Fraud Risks: A practical guide

Presented by

Olivia Burren
Risk Consultant, Lockton Companies LLP

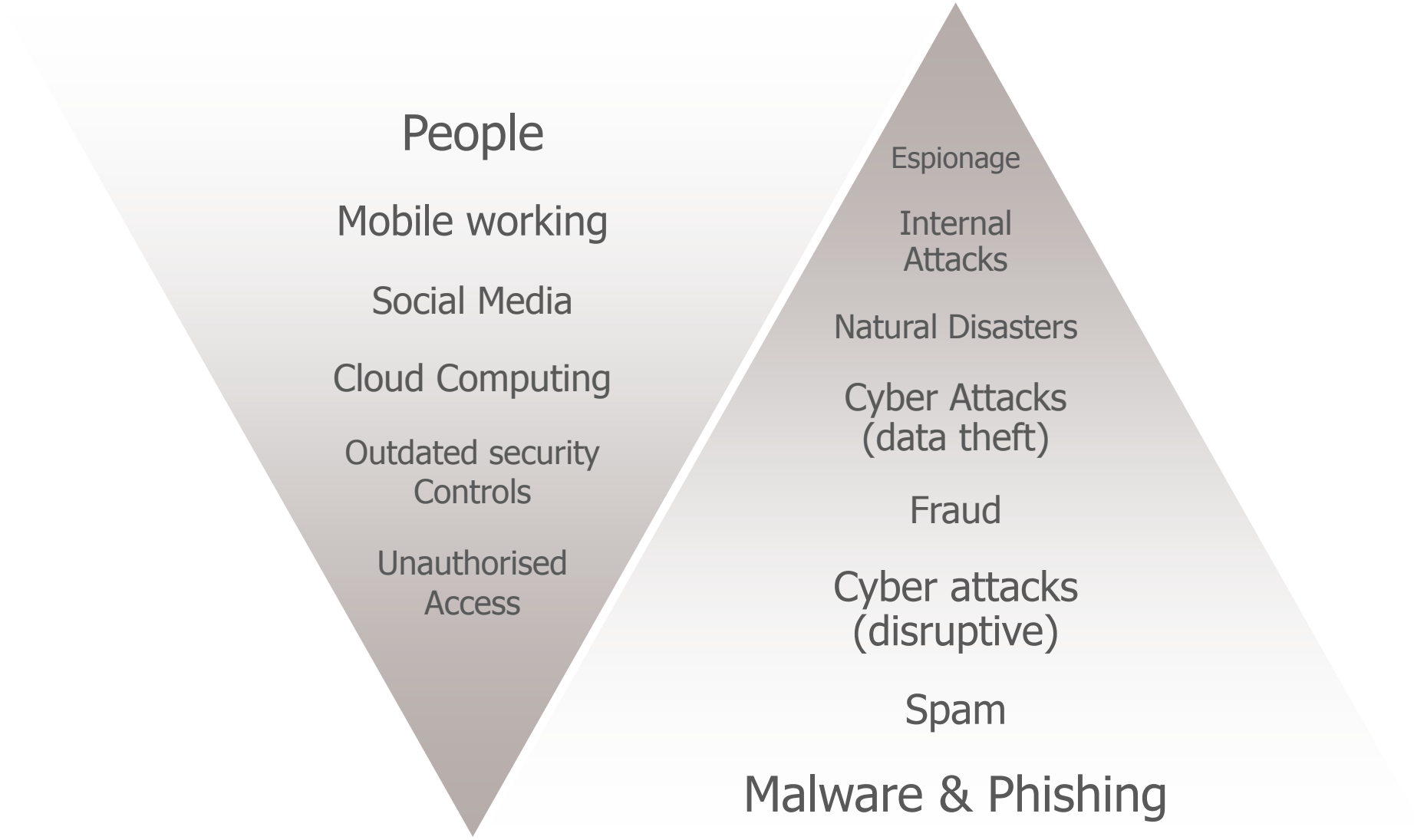
Calum MacLean
Risk Manager, Lockton Companies LLP

The Same Old Story?



Risks: a refresher

Vulnerabilities & Threats



Regulatory issues

What the new EU GDPR means in 1 minute

The EU GDPR will increase privacy for individuals and give regulatory authorities greater powers to take action against businesses that breach the new laws. Here's what it means for your business:

Tough penalties:
fines of up to

4% of annual global revenue

or

€20 million, whichever is greater.

The regulation also applies to **non-EU companies** that process personal data of individuals in the EU.

Reproduced courtesy of IT Governance Ltd
www.itgovernance.co.uk/data-protection/eu-gdpr-infographic.aspx

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?

96% data leaks are inadvertent

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

People Risks

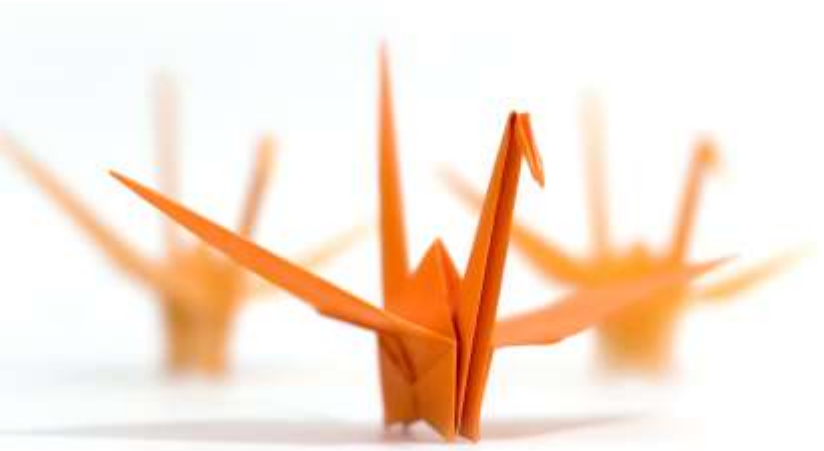
Carelessness, stupidity, malice?

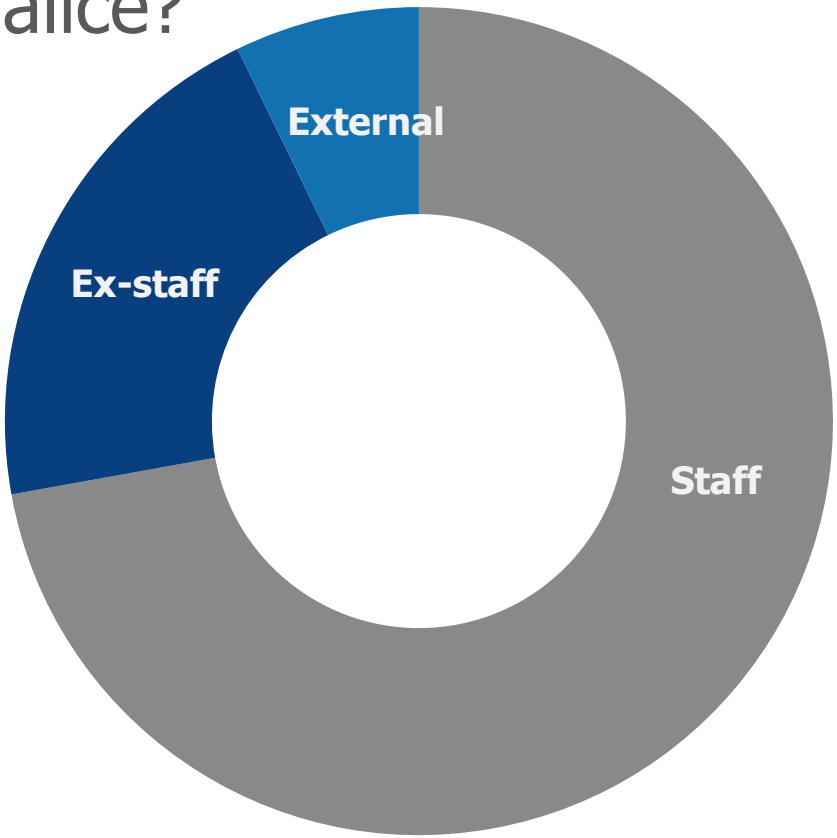
- Emails
- Careless conversations
- Remote working
- BYOD

Shared passwords

Social media

Criminal intent





Reducing risks - people

Recruitment: references & vetting

Regular, practically-focussed, refresher training

Systems & Procedures

Supervision

Systems

Frauds & Scams

Identity fraud

Social Engineering

Phishing

Trojans

Vishing

Invoice Hijacking

Targetting Identity Fraud

Client & Transaction Vetting

Social engineering

Risk Awareness

Training

Transaction – client vetting

Social Media

Phishing

Phishing


2
TAKE 2 (GLANCES) BEFORE
YOU CLICK THROUGH
www
If you suspect the message is phishy, just delete it.

Vishing

Telephone call fraud

Impersonating bank staff

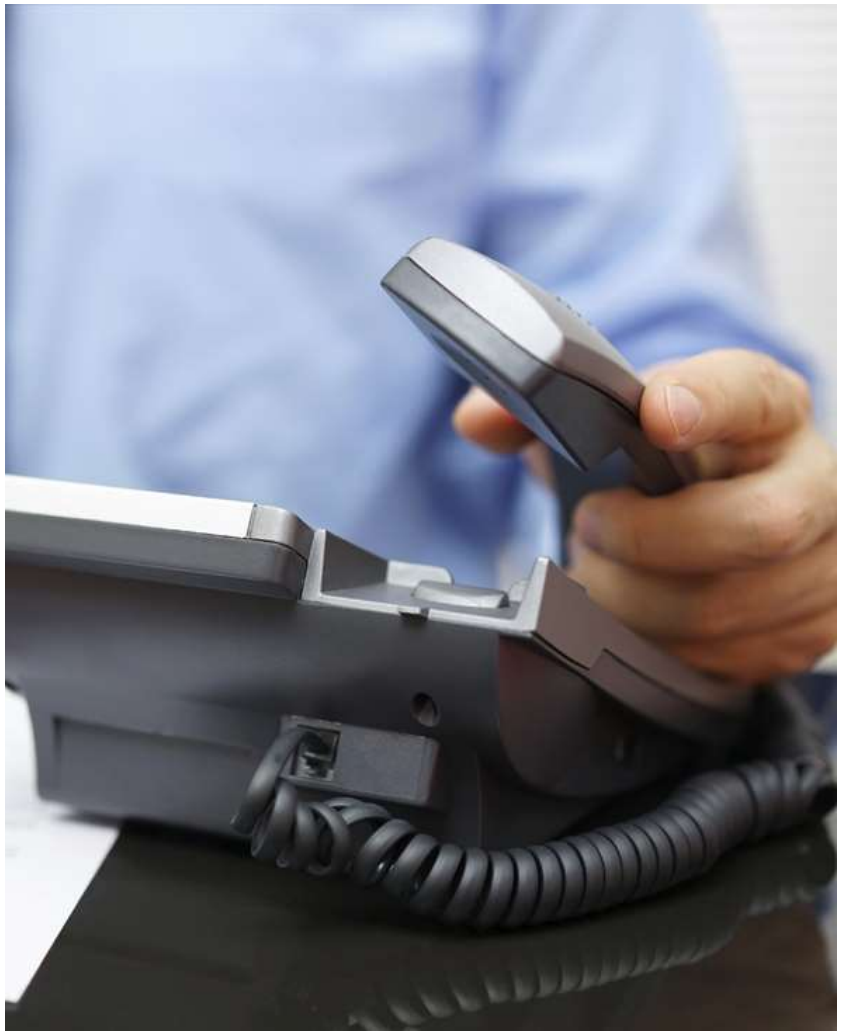
May identify ‘suspicious transactions’

Likely to know of real genuine activity on your account also

Will suggest urgency

Will ask for detailed security information

Vishing risk mitigation



HANG UP immediately

Use only the **OFFICIAL BANK NUMBER**

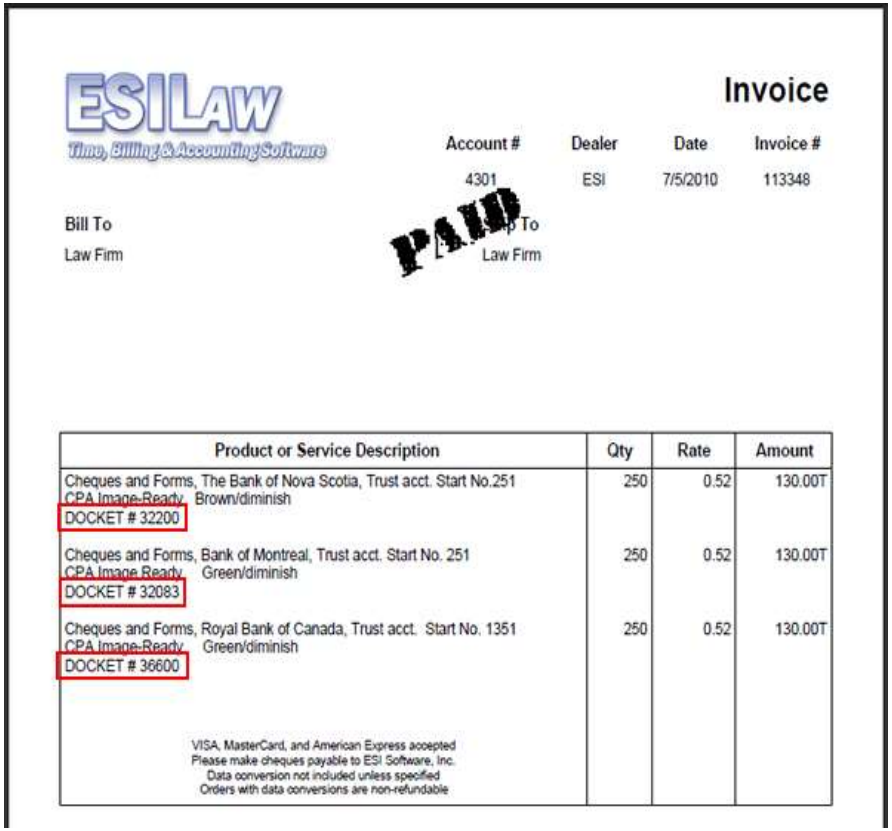
Use a **DIFFERENT TELEPHONE**

EDUCATE YOUR STAFF on the risks

Website hacking

Invoice Hijacking

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



ESILAW
Time, Billing & Accounting Software

Invoice

Account #	Dealer	Date	Invoice #
4301	ESI	7/5/2010	113348

PAID

Bill To
Law Firm

Ship To
Law Firm

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

Cost of data breach: UK

The average total cost of a breach for a UK company in 2015 was £2.37m

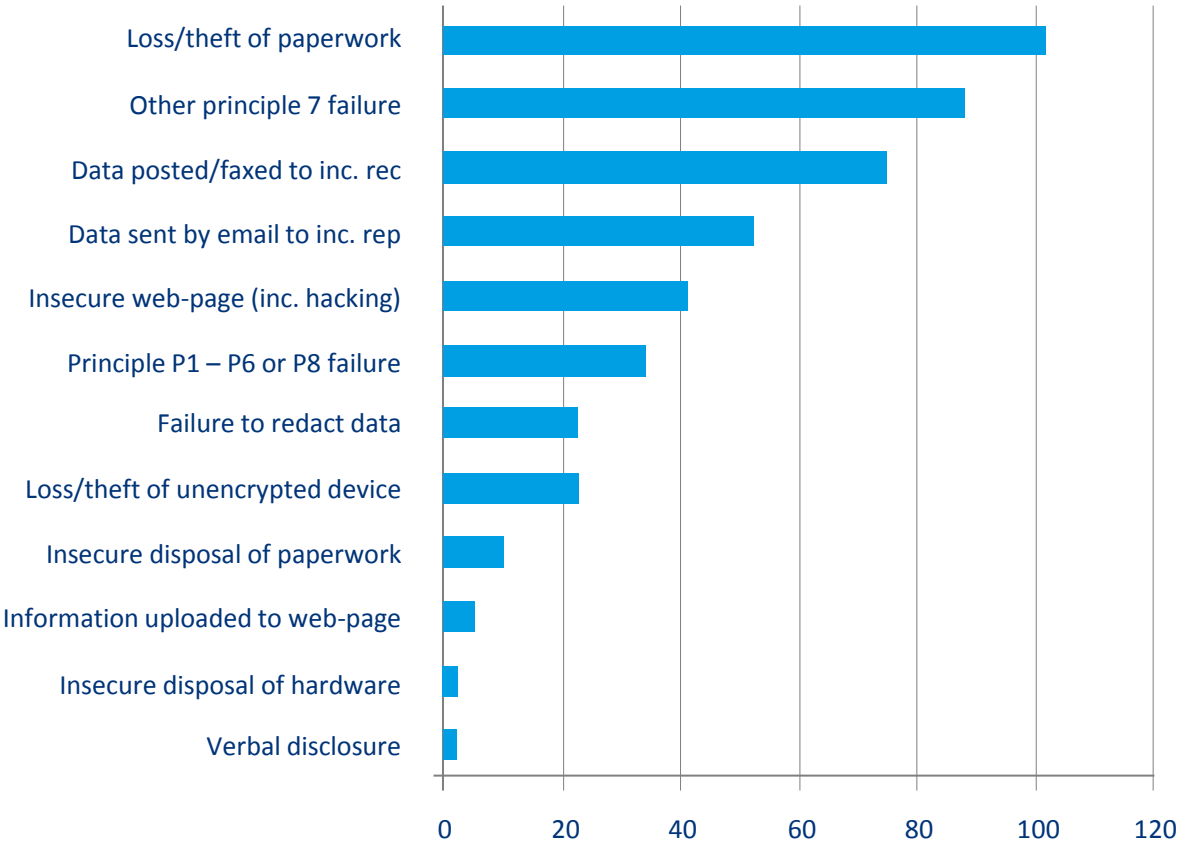
Lost revenue following a data breach increased from £950k to £1.07m in 2015

The average cost per lost record increased to £104 from £95

Malicious attacks are more costly than incidents involving human error (£123 vs £90)

Source: Ponemon Institute LLC - 2015 Cost of Data Breach Study

Breach types 2014-15



Courtesy of the ICO

Recent ICO fine

Prodial Ltd (£350,000 February 2016)

- Prodial Ltd, a lead generation firm responsible for over 46 million automated nuisance calls.
- 1,122 people complained to the ICO about the automated calls which played recorded messages relating to PPI claims.
- Found to be in breach of Regulation 19 of the Privacy & Electronic Communications (EC Directive) Regulations 2003 - PECR, which states that:
- Largest ever fine by the ICO.

LOCKTON

- Year 2014 data breach
- 99,998 employees' personal details leaked by a disgruntled internal auditor
- Bank details, NI numbers, salary details
- He was subsequently jailed
- 6000 staff now suing the supermarket for failure to look after the data

Alan Calder CEO of IT Governance says
"Heads of HR need to be as concerned about data security as heads of IT"

Future vulnerabilities and emerging trends

- The Internet of Things and Interconnectivity
- Supply chains
- Industrial espionage
- Ransomware

LOCKTON

Cyber Security V Insurance Premium

Insurable losses

- Breach Event Costs
  - Notification costs - where required by law
  - Legal, forensic, public relations, call centre, credit / ID protection
- Loss of Digital Assets
  - Costs incurred to restore data & software
- Non-physical Business Interruption
  - Loss of income and extra expense following a non-physical event - DDoS
- Cyber Theft
  - Losses arising directly from security breaches where funds are transferred to a false account
- Cyber Extortion
  - Costs to end a security threat or pay a ransom demand
- Third Party Costs
  - Civil suits - defence costs and damages
  - Regulatory actions - defence, civil fines and penalties
- Payment Card Industry Data Security Standards (PCI DSS)
  - Liability arising from breaches of PCI DSS
- Reputational Harm
  - Loss of income following a breach or business interruption or social engineering

Data Security & Privacy Matrix	Professional Indemnity Insurance	Cyber Insurance	Crime
First Party Data Security & Privacy			
Breach Response Costs including:	Not Covered	Covered	Not Covered
- Specialist legal expenses	Not Covered	Covered	Not Covered
- Forensic expenses	Not Covered	Covered	Not Covered
- Notification costs	Not Covered	Covered	Not Covered
- Public relations expenses	Not Covered	Covered	Not Covered
- Credit & ID monitoring costs	Not Covered	Covered	Not Covered
Data Restoration Costs	Not Covered	Covered	Not Covered
Network Business Interruption	Not Covered	Covered	Not Covered
Cyber Extortion	Not Covered	Covered	Covered
Cyber Theft	Not Covered	Limited Coverage	Covered
Third Party Data Security & Privacy Liability			
Liability to 3rd parties arising from security & privacy breaches	Should be covered, where arising out of professional business, but questions may arise regarding coverage intent and investigation costs.	Covered	Not Covered
Liability to employees and partners arising from security & privacy breaches	Not Covered	Covered	Not Covered
Regulatory defence, civil awards, fines & penalties	May be limited cover.	Yes, to the extent insurable by law	Not Covered

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

Thank you for listening

CPD Hours: 1 hour

Contact us for CPD Code