



Institute of Internal Auditors
WELSH DISTRICT SOCIETY

RISK & REWARD

By Steven Connors, Partner

HW Controls & Assurance - Part of Haines Watts Chartered Accountants.

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

Standards

- ❑ Why do we need them?
- ❑ How should we apply them?

The Usual Suspects

- ISO 17799 /
 - ISO 27002
- SAS 70
- ISO 27001 (BSI 7799)
- ITIL / ISO 20000
- PCI
- GSi/CoCo
- COBIT
- GASSP
- IPR
- Data Protection Act

Why do we need them?

- Information is an asset and as such has a value
- We need to protect our information assets
 - Otherwise
- A business opportunity – for the unscrupulous!

Our Information Assets

- ❑ What are they – Only you can decide!
- ❑ Identity?
- ❑ Trade secrets?



How should we apply them?

- ❑ Diligently
- ❑ Align our Information Security Strategy with our Corporate Strategy
- ❑ Consistently

Why Bother?

- MOD
- HMRC
- EDS
- PA Consulting
- Deloittes
- DEFRA

It Affects Us All

- ❑ French police probe Sarkozy bank fraud
- ❑ Discs posted from HM Revenue and Customs offices in Tyne and Wear, but never turned up at their destination – the National Audit Office.

.

TV presenter Jeremy Clarkson has lost money after publishing his bank details in his newspaper column.



Clarkson now says of the case: "Contrary to what I said at the time, we must go after the idiots who lost the discs and stick cocktail sticks in their eyes until they beg for mercy."

Does it matter?

- ❑ Lost data costs!
 - ❑ Damage to reputation
 - ❑ Money
 - ❑ Jobs
 - ❑ Identity

Impacts

- ❑ “Data breaches cost UK companies an average of £47 for every record lost.” Source, J Oates, The Register, 25th Feb 2008.
- ❑ New boss for HMRC after data slip
- ❑ Data loss firm contract axed

Identity Fraud Costs!

- Identity fraud cases up by nearly 50 per cent, according to latest Experian figures – Majority of cases discovered when people check their credit reports
- UK banking fraud soars in 2008 – Apacs reports overall losses of £300m in the first six months
- Two missing computer discs containing the personal details of 25 million people could be worth up to £1.5bn to criminals. Vince Cable, Lib Dems.

Data on the Open Market

- ❑ Identity is the key
- ❑ 'relatively static data' is the objective
 - ❑ name, DOB, sex, address, is good;
 - ❑ NI no. is great;
 - ❑ account details are the holy grail!
- ❑ criminals will pay for quality data

- "In the fraud underworld the quality of data directly impacts the flexibility with which they can use it," The more data you have around a subject the more different ways you can use that to commit fraud." — Andrew Moloney, financial services market director for RSA Security.

Growth of e-commerce

- ❑ Internet shopping could account for half of Britain's £300 billion-a-year retail market by as early as 2018
- ❑ IMRG believes that consumers have spent a record £53 billion online this year, up 75 per cent on last year and a market share of 17 per cent.

- ❑ Four factors have come together at once:
 - ❑ familiarity;
 - ❑ availability;
 - ❑ confidence on the part of consumers; and
 - ❑ investment on the supply side.

ISO/IEC 17799:2005 Threat Management

- security policy;
- organisation of information security;
- asset management;
- human resources security;
- physical and environmental security;
- communications and operations management;
- access control
- information systems acquisition, development and maintenance;
information security
incident management;
business continuity management;
- compliance.

Tying the Corporate & Security Strategies

- The control objectives and controls in ISO/IEC 17799:2005 are intended to be implemented to meet the requirements identified by a risk assessment.
- One size does not fit all – made to measure is the key!

Considerations

- ❑ Controls cost money
- ❑ Monitoring costs money
- ❑ Updating costs money
 - ❑ Lean process – apply only what is necessary
 - ❑ Consistency

Compliance with good practise V's ISO 17799 accreditation

- ❑ Cost – money and resources
- ❑ Benefit – commercial/operational
- ❑ Value – piece of mind

In a Nutshell

The good practice International Standard for Information Security Management (ISO27001) defines the process requirements for such a system as:

- ❑ understanding an organisation's information security requirements and the need to establish policy and objectives for information security;
- ❑ implementing and operating controls to manage an organisation's information security risks in the context of the organisation's overall business risks;
- ❑ monitoring and reviewing the performance and effectiveness of the ISMS; and
- ❑ continual improvement based on objective measurement.

ISO 17799 to PCI SS to GSi/CoCo

- While the PCI Standard was not written to map specifically to ISO 27001, ISO 17799, CobiT or any other existing framework, it sits clearly within the ISO 17799 (now ISO 27002) framework and organisations that have implemented an ISO 17799 ISMS should be able, with minor additional work, to also demonstrate their conformance with the PCI standard and GSi.

Blatant Plug!

Steven Connors, Partner
HW Controls & Assurance

swconnors@hwca.com

www.hwias.co.uk