

Did I really mean to do that?

Donna Goddard, Executive Director,
Sarah Lowman, Associate
Information Security, Morgan Stanley

First Thoughts

- Why is Information Security important?
 - For companies
 - Data Protection Act
 - Client Confidentiality requirements
 - Intellectual Property
 - Franchise Risk
 - For you as individuals
 - Things to consider
 - Limited control on visibility
 - > Who by
 - > How long
 - Personal security
 - > Hackers / Organised crime
- Ultimate impact

Regulatory, Ethical & Privacy Implications

- Increased regulatory sanctions
- Data loss events
- Reporting obligations
- Complexity of Privacy laws globally

Increased Regulatory Sanctions & Data Loss Events

- **UK Data Protection regulator** can impose fines up to £500K.
 - The FSA fined Zurich Insurance Plc (“Zurich UK”) £2,275,000 (reduced by 30% from £3.25m due to co-operation), for losing personal data on 46,000 customers. This is the largest fine for a data security breach in the UK.
 - **Switzerland** can result in a custodial sentence and a large fine (even if no malicious intent)
 - Other European regulators have increased or have new powers to impose sanctions e.g. Hungary.
- **US - Complex combination of Federal vs. State**
 - (Suit Under Massachusetts Data Security Regulation): in May 2011 a surveillance camera showed that a tape containing unencrypted personal information was *inadvertently* thrown away by the evening cleaning crew at a bank and, according to the Massachusetts’ Attorney General’s office, most likely was incinerated by the bank’s waste disposal company. Even though there was no evidence consumers’ personal information was acquired or used by an unauthorized person or used for an unauthorized purpose as a result of the breach, the bank was required to pay a civil penalty of \$7,500 and make formal assurances that it would comply with the Massachusetts regulation and its own written security policies

Reporting Obligations

- **Germany** –
 - There is an express legal requirement to notify breaches of certain types of data, such as bank data, sensitive data or data subject to “professional secrecy”.
- **Sweden** –
 - The Data Controller is obliged to inform the Data Subjects of the breach.
- **Ireland** –
 - Irish Personal Data Breach Code of Practice recommends, (without formal legal obligation), that all incidents which personal data has been put at risk be reported to the Data Protection Commissioner.
- **UK** –
 - ICO encourages notification
- **US – Federal versus State**
 - State breach notification laws typically contain either a “harm-based” or “non-harm-based” threshold:
 - Harm-based trigger: notification is not required unless it is determined that there is a reasonable likelihood that the unauthorized access or acquisition will result in harm to the affected individuals
 - Non-harm-based trigger: notification must be provided regardless of whether there is any evidence that the incident is likely to result in harm (prominent examples = NY and CA)
 - Government Agency Notification Requirements - A number of states require entities to notify a state agency when notifying residents of that state of a breach incident (e.g. State Attorney General, Consumer Protection Authority or the State Police)
 - Indiana, Louisiana, Maine, Maryland, Massachusetts, New Hampshire, New Jersey, New York, North Carolina, Puerto Rico, Virginia (regardless of the number of affected individuals)
- There may be further notification obligations to other regulators e.g. FSA, FINMA, FED, OCC amongst many others

What's next?

- EU Data Protection Directive strengthening
- Advancement in technology, including mobile technology, virtualization and cloud computing
- Social Networking Sites
- New Cookie Legislation

When it all goes wrong

- Poor testing?
 - Foreign and Commonwealth Office
 - Citibank Credit Card
 - RSA
- Encryption of personal data
 - Child benefit
 - Nationwide laptop

Social Networking, the good, the bad & the ugly

**Jake Davis named as suspected hacker
Tophary by UK police**

Facebook in new privacy row over facial recognition feature
Social network turns on new feature to automatically identify people in photos, raising questions about privacy implications of the service

by Graham Cluley on July 3
FILED UNDER: Data loss, Law
British police have tor
teenager they arrest
in relation to the Lulz
hacking groups.

IT Security & Network Security News
Using Facebook to Social Engineer Your Way
Around Security

By: Brian Prince
2009-04-07
Article Rating: ★★★★★ / 7
There are 1 user comments on this IT Security & Network Security News & Reviews story.

A penetration test by Netragard at an energy company highlights how hackers can use Facebook, LinkedIn and other social networking sites as part of phishing schemes. In the test, Netragard used social engineering to get its hands on information that could have been used to compromise critical systems at the company. Addressing this security issue means having smart policies about what employees can and cannot do on the Web.

The most important part of an attack isn't always a vulnerability; sometimes it's the user's trust.

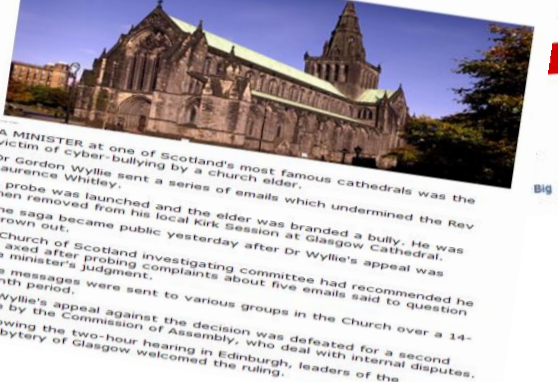
This was certainly the case during an authorized penetration test at an energy company conducted by security vendor Netragard. Looking for a way inside the customer's defenses, the vendor turned to Facebook, bolstered by information on work experiences of employee of that company, and began "friending" users on the Web.

What the Facebook "friends" didn't know was that this was all part of a long con—a bit of social engineering used to lull the employees into giving up their credentials more easily. The simulated attack underscores both the importance of having sound policies on employee use of sites like Facebook, LinkedIn and MySpace and the challenges of authenticating users on the Web.

"Before the advent of social networks, criminals were able to access your employees through things like spam, or maybe they could call them up and social-engineer them," said Adriel Desautels, CTO of Netragard. "But sites like Facebook and MySpace and LinkedIn and all these different sites [give] criminals the ability to bypass just about any security technology you have in place and gain direct social access to your employees."

Rate This Article:

Poor Best



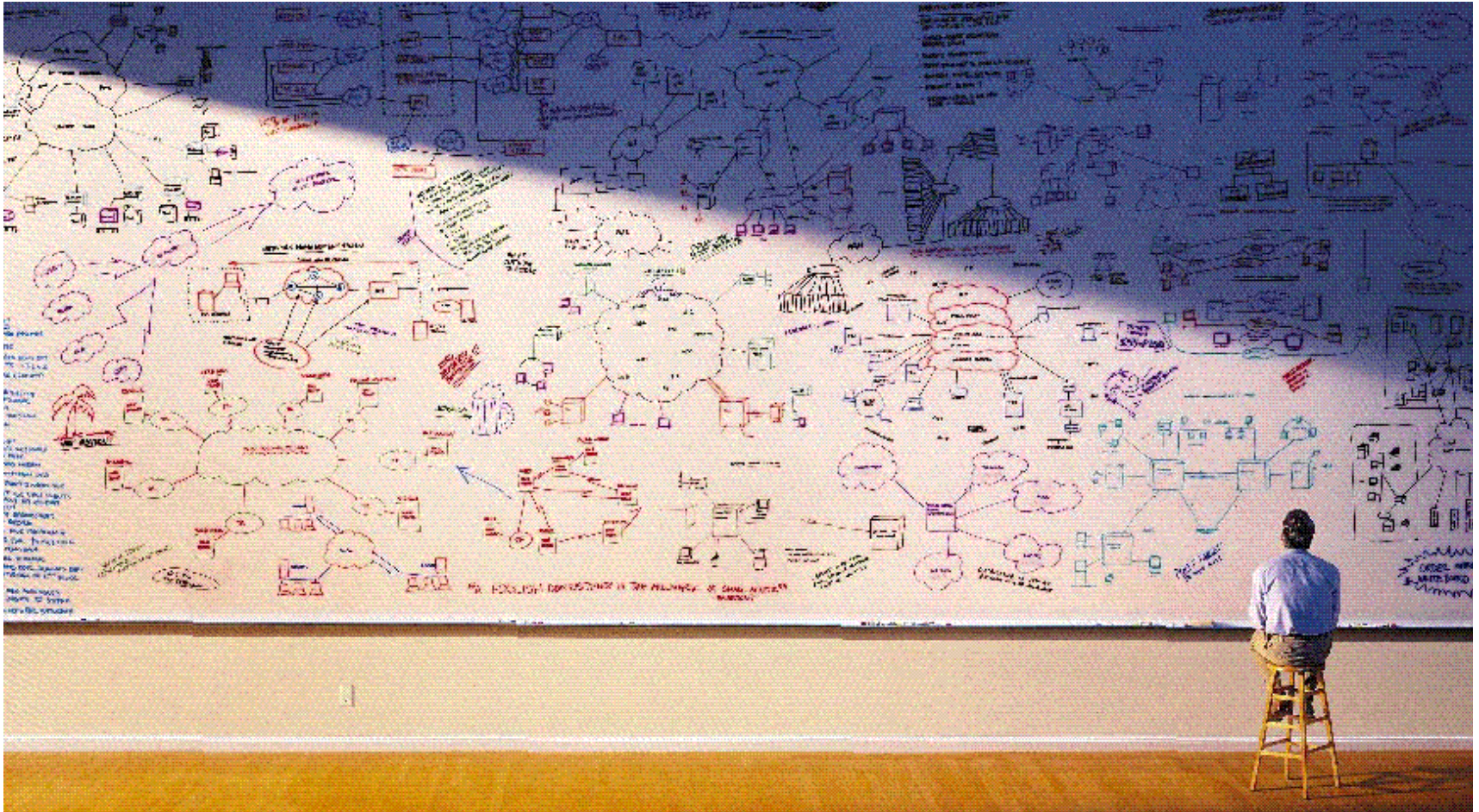
Social Networking, the good, the bad & the ugly

- The Good
 - What's the biggest Internet danger? That we concentrate on the dangers and forget the positives:
 - Entertaining and having fun
 - Expressing and sharing stories
 - Engaging and changing the world
 - Educating and helping peers
- The Bad
 - Privacy Implications / Identity theft
 - Phishing / Spear phishing
 - Social Engineers
 - Malware
 - International Cyber-Crime
- The just plain ugly!
 - Property damage/Anti-Social behaviour
 - Online Threats
 - Cyber-Bullying
 - Criminal sanctions











To Sum Up

- If something seems too good to be true it generally is
- Don't be a twit when you twitter, you owe it to yourself to protect yourself online
- Social Networking sites and the Internet are like any other technology
 - Adjust the privacy settings of social network sites so you aren't conducting your entire life as an outside broadcast with everyone in the world
- Test, test and test again

Questions



Campus Programmes – Glasgow

Division	Analyst Programme Full Time	Internship Programme 13 Weeks	Industrial Placement 48 Weeks
Operations	 *		
Finance			
Fund Services	 *		
Technology			

* Operations and Fund Services Analyst programmes currently full for 2012

Recruiting - Next Steps

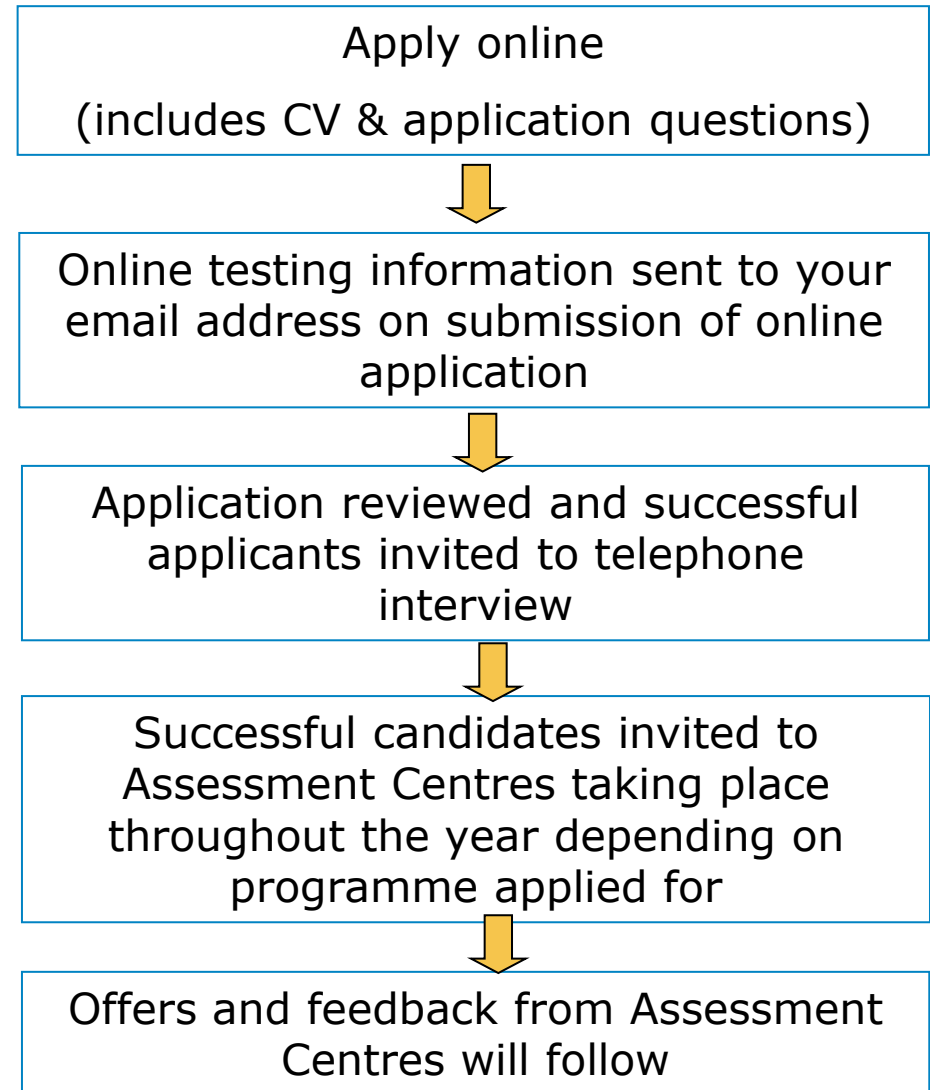
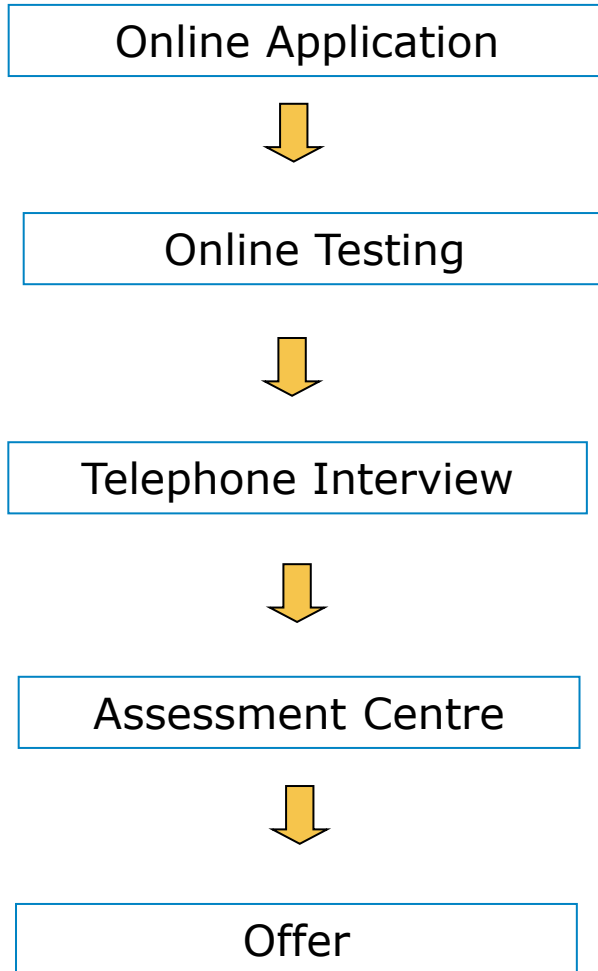
START DATE	DIVISION	ROLE	CLOSING DATE
Summer 2012	Finance	Full Time Analyst	30 th Dec 2011
Summer 2012	Finance	Summer Analyst	31 st Jan 2012
Summer 2012	Fund Services	Summer Analyst	31 st Jan 2012
Summer 2012	Operations	Summer Analyst	31 st Jan 2012
Summer 2012	Operations	Industrial Placement	31 st Jan 2012
Summer 2012	Technology	Full Time Analyst	24 th Feb 2012
Summer 2012	Technology	Industrial Placement	24 th Feb 2012

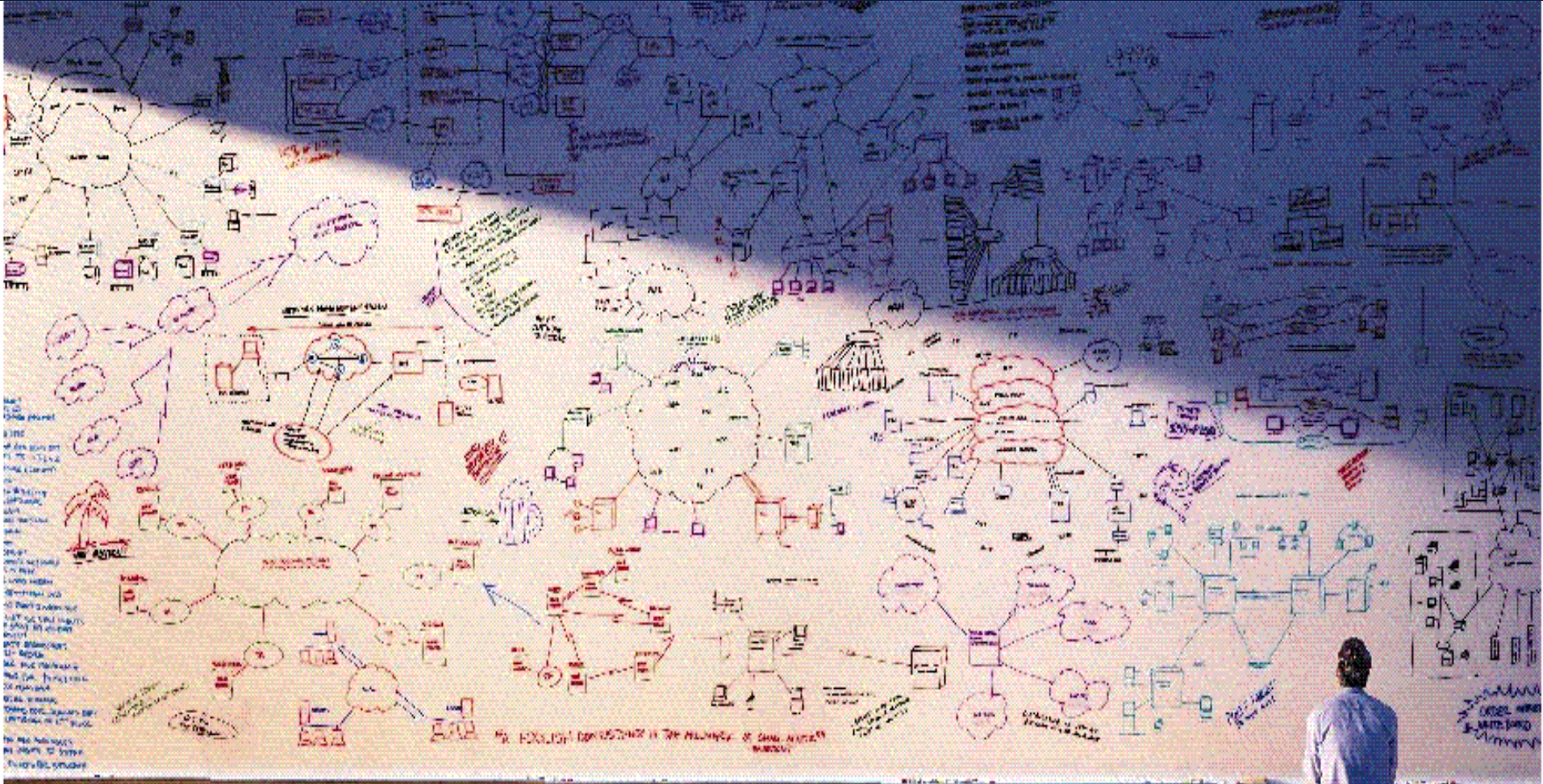
Roles starting February 2013 will be advertised from Spring 2012

Recruiting Website: www.morganstanley.com/glasgow

Apply online via application form

The Selection Process





Any questions and thank you!

Appendix

Appendix 1: Review of the Data Protection Directive

- The current European Data Protection Directive is outdated in light of recent technological developments.
- Draft legislation is expected in Autumn of 2011 and will be based on the following four “pillars”:
 - **“Right to be forgotten”** – A right for the individual to withdraw consent to data processing, with the burden on data controllers to demonstrate a legal basis for processing and retaining data;
 - **Transparency** – Enhancing existing transparency requirements, probably by requiring the provision of greater (and more intelligible) information about what data is collected, individuals’ rights, third party use of data, associated risks and details of the applicable data protection authority;
 - **“Privacy by default” and “Privacy by Design”** – Rules to ensure that default privacy settings, (i.e. opt out rather than opt in) and the design of systems, prevent unfair, unexpected or unreasonable processing of personal data;
 - **Protection regardless of data location** – EU data protection laws to apply irrespective of the location of data processing and the means used by the controller to process data, i.e. giving them extra-territorial effect.
- Drive for consistency across European jurisdictions

Appendix 1: Review of the Data Protection Directive (Cont)

- Other countries are proposing to adopt the European approach, e.g. South Africa, India and Turkey, so European privacy/data protection issues can no longer be looked as only being relevant in the EU.
- Legal requirements to notify of security breaches are likely to be implemented in member states in the future.
- Privacy By Design/Default is going to have significant impact on technological development.
- The new Data Protection Directive will attempt to harmonise the discrepancies between how member states interpret and implement the law, but this will be challenging due to cultural differences and divergent views on privacy vs. public good.
- Rapid technological advancement is likely to raise further data protection/privacy issues resulting in the law having to continue to “play catch up”.

Appendix 2: Further Reading & Useful Links

• Useful Links

- Sign up for alerts from the SANs Organisation
 - <http://portal.sans.org/>
- Morgan Stanley's Glasgow Office
 - www.morganstanley.com/glasgow
- Information Security
 - Get Safe Online – User friendly non profit site, offering guidance and articles on how to protect yourself online:
 - <http://www.getsafeonline.org/>
 - Test your ability to detect online threats:
 - <http://threattest.knowthenet.org.uk/>
 - Download the Sophos 2011 threat report:
 - <http://www.sophos.com/en-us/security-news-trends/security-trends/security-threat-report-2011.aspx>
 - Read the Government's National Security Strategy:
 - http://interactive.cabinetoffice.gov.uk/documents/security/national_security_strategy.pdf

• Useful reading list

- Zen and the Art of Information Security – by Ira Winkler
- The Art of Intrusion – Kevin Mitnick
- The Art of Deception – Kevin Mitnick
- Secrets and Lies – Bruce Schneier