graphic from wordle.net

Report of the
Data Protection Review Group

March 2010

Contents

1. Summary

1.1. The Data Protection Review Group was established by the Minister for Justice, Equality and Law Reform Mr. Dermot Ahern T.D. to examine whether legislative changes were needed to address the issue of data breaches, with particular reference to mandatory notification of breaches to data subjects. The Group following an initial consideration, identified eight regulatory options. It published a consultation document in September 2009 looking for views on these options. Following the closure of the consultation period in October 2009 and further consideration the Group now recommends that:

1. Legislation should provide for a general offence by a data controller of deliberate or reckless acts or omissions in relation to the data protection principles – including contraventions of the security principle in relation to data breach incidents. This would complement the existing offence under the Data Protection Acts for failure to comply with an Enforcement Notice issued by the Data Protection Commissioner (DPC)-including an Enforcement Notice directing a data controller to inform individuals of a data breach affecting them.

2. The reporting obligations of data controllers in relation to data breaches should be set out in a statutory Code of Practice as provided for under the Data Protection Acts. The Code, broadly based on the current guidelines from the DPC, should set out the circumstances in which disclosure of data breaches is mandatory. Failure to comply with the disclosure obligations of the Code could lead to prosecution by the DPC.

3. The Code should be reviewed on a regular basis by the DPC and amendments submitted to the Minister as necessary to keep the legislation current.

4. The DPC should continue to develop his investigation and audit activities in a targeted way, with a particular focus on organisations which hold sensitive personal data, in compliance with emerging risk-based approaches to enforcement.

5. Legislation should provide for the timely publication of the outcome of such DPC audits, as an aid to good practice and in the interests of transparency.

6. The DPC should continue to develop public awareness activities in this area.

1.2. While the work of the Group has been under way there have been substantial developments in the EU, internationally with industry groups and in Ireland with the High Level Group on Business Regulation. Some of these developments are relevant to the work of the Group and are taken into

account in the recommendations of the Group. In particular, the Group considers that its recommendations are consistent with developments at EU level. The timing of any proposed legislation would be influenced by the pace of these developments – predominantly those under consideration by the EU Commission. It is probable that a review of the existing Data Protection Directive now underway by the Commission will give rise to proposals for a new or amending Directive either later this year or during 2011. The indications are that such a new proposal would address many of the issues covered by the work of the Group, in particular providing for some form of mandatory notification to data subjects in cases of data breach. The Group took note of the enhanced competence available to the Commission in this area following the coming into force of the Lisbon Treaty.

1.3. The Group took account of the adoption by Government, in March 2008, of a target to reduce the administrative burden of regulation on business by 25%, and of the work of the High Level Group on Business Regulation. The Group was concerned that any proposals for new regulation and enforcement regimes should be targeted in an effective manner. The Group is satisfied that its proposals are a reasonable and pragmatic combination of principle-based regulation and risk-based enforcement and are in line with national, EU and broader international level developments.

2. Introduction

2.1. The Minister for Justice, Equality and Law Reform, Mr. Dermot Ahern T.D., established the Data Protection Review Group in November 2008 to examine whether legislative changes were needed to address the issue of data breaches, with particular reference to mandatory notification of breaches to data subjects.

2.2. The Group's **terms of reference** are:

a. Legal issues

i. Consider whether Irish Data Protection legislation needs to be amended to deal with data breaches.
ii. Assess the effectiveness of existing legislation in this context, including the impact of mandatory reporting legislation where it has been introduced.
iii. Assess the likely impact of the scope and timing of the forthcoming ePrivacy Directive and next EU Data Protection directive and other relevant international legislative developments.
iv. Describe the range of options in existing legislation within EU and with competing non EU states.
v. Consider the potential formats of mandatory reporting.
vi. Consider the role and level of penalties in any mandatory regime.

b. Technical issues

i. Definition of "breach" in the context of how organisations' use of technology is changing
ii. Assessment of the assortment of devices and locations holding data now.
iii. Assessment of whether the same mechanisms should apply to paper and electronic media in any suggested change.
iv. Attempt to foresee unintended consequences in the light of the rapid evolution of technology and business practices.

c. Regulatory issues

i. Assess the prevalence of the data breach problem and level of existing reports.
ii. Assess any empirical evidence that Data Protection legislation informs industrial location decisions.
iii. Consider whether any changes bear on Public and Private sectors equally.
iv. Assess how to establish the threshold of seriousness - in some cases a very small number of records could potentially cause substantial harm.
v. Balance the potential effectiveness of any proposed change against increasing the costs of doing business in Ireland - the Group should, insofar as possible, ensure that its deliberations equate to a Regulatory Impact Analysis.

Should the Group form a view that any interim measures are available that would help the overall objective of reducing the risk of data breaches then they are encouraged to make an interim report to the Minister.

2.3. **Membership**:

Chairman: Mr. Eddie Sullivan (former Secretary General, PSMD, Department of Finance),
Mr. Paul Carroll (Department of Social and Family Affairs),
Professor Robert Clark (formerly of the School of Law, UCD),
Mr. Alec Dolan (Department of Justice, Equality and Law Reform),
Ms. Isolde Goggin (expert on Regulatory Impact Assessment),
Mr. Billy Hawkes, (Data Protection Commissioner),
Mr. Dave Ring (CMOD, Department of Finance) - replaced on retirement by Mr. John Brennan,
Mr. Tony McGrath (Department of Enterprise, Trade and Employment),
Mr. Roger O'Connor (Department of Communications, Energy and Natural Resources)
and Ms. Noreen Walsh (Department of Justice, Equality and Law Reform)

Mr Mark Holland (Department of Justice, Equality and Law Reform) is Secretary to the Group.

2.4. The Group, which met eight times, proceeded by way of an initial call for submissions, a series of meetings working through the terms of reference, a consultation exercise among group members and extensive desk research. The Group published a consultation paper in September 2009 which identified a number of options and sought views on them. Appendix 2 lists the submissions received Following the closure of the consultation there has been some follow up work, in particular on clarifying the likely pace and scope of EU developments, where a consultation exercise has recently concluded. Pending the outcome of the work of the Group, the Department of Finance issued revised guidelines on Data Protection for the Public Service and the Data Protection Commissioner (DPC) updated his Office's Guidelines on best practice. Both documents strongly recommend breach disclosure to data subjects, where appropriate, as an effective harm reduction mechanism. (http://www.dataprotection.ie/viewdoc.asp?DocID=901&ad=1.)

2.5. The Consultation document discussed in broad terms a number of aspects of the topic and eight regulatory options were identified. Interested parties were asked to provide comments by October 31 2009 to assist the Group reach a balanced conclusion on how Ireland should address the issue of the most appropriate regulatory response to data breaches. While the work of the Group was going on devices continued to be lost or stolen. Perhaps encouragingly the most recently widely reported instances (Bord Gais and HSE) showed a greater degree of encryption in place than would have been the case previously. Both were reported directly by the organisations concerned to either the DPC or An Garda Síochána.

Breach Definition

2.6. A data breach is defined by the EU Commission (in the ePrivacy Directive – 2009/136/EC amending 2002/58/EC) as "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed in connection with the provision of a publicly available electronic communications service". This definition is broadly the same as that used in breach notification legislation in existence in most states in the United States. A data breach can happen for a number of reasons, including:

- loss or theft of data or equipment on which data is stored;
- inappropriate access controls allowing unauthorised use;
- equipment failure;
- human error;
- a hacking attack;
- access where information is obtained by deceit;
- unforeseen circumstances.

Appendix 3 provides an indicative list of a variety of breaches and responses.

Current Legislative Framework

2.7. The Data Protection Acts 1988 to 2003 impose obligations on organisations ("data controllers") that process personal data. "Personal data" and "processing" are defined very broadly to cover any information that can be related to a living individual (a "data subject") and anything done with that information. The principles governing the processing of personal data are that such data should be:

- obtained and processed "fairly"(usually involves consent);
- collected for a specified purposes;
- not be disclosed to other parties;
- kept safe and secure;
- kept accurate and up-to-date;
- be relevant and not excessive;
- not be retained for any longer than necessary;
- available to the individual concerned on request.

2.8. None of the principles is given any special status over the others. A data controller is obliged to adopt "appropriate security measures". These are defined in the legislation as being "appropriate to (i) the harm that might result from unauthorised or unlawful processing, accidental or unlawful destruction or accidental loss of, or damage to, the data concerned, and (ii) the nature of the data concerned". The data controller "may have regard to the state of technological development and the cost of implementing the measures". The data controller must take "reasonable steps" to ensure that employees are aware of and comply with the security measures in place.

2.9. Under existing law, there is no specific legal obligation imposed on a data controller to inform either a data subject or the DPC of an incident involving the loss or improper disclosure of personal data. Consequently, there is no legal penalty for deciding not to inform either the subject or the DPC. Breach reporting itself is not one of the data protection principles but the requirement to report to the data subject forms part of the guidance to support the security principles. The DPC issued breach notification guidelines in 2009 which recommends that, as soon as a data controller becomes aware that personal data for which it is responsible has been compromised, it should immediately notify the DPC. These guidelines do not have the force of law. The Act provides that the DPC can give guidance in different forms, including the issue of general guidance on good practice. It is on this basis that the present guidance on data breaches has been issued.

2.10. The Data Protection Act provides for Ministerial approval of Codes of Practice prepared by the DPC. Such Codes, once approved by the Minister and by a resolution of both Houses of the Oireachtas, would have the force of law. This method has not been used in this context and in the Group's view could form the basis of a regulatory mechanism.

2.11. Once the DPC becomes aware of a security breach, he can issue an Enforcement Notice to the organisation concerned requiring it to notify affected individuals, if this has not already been done. The DPC can also use his extensive audit and investigation powers to carry out a detailed examination of the level of data security in the organisation. This can provide the basis for further remedial measures which can also be prescribed in an Enforcement Notice. Failure to comply with such an Enforcement Notice is an offence which can be prosecuted by the DPC. In practice, the DPC has not had to issue such Notices to achieve compliance in cases of data breaches. Organisations would be aware that such a Notice could be issued and followed by a prosecution if not complied with. A broadly similar approach, with some variations, is taken by other EU Data Protection Authorities.

Telecommunications Framework

2.12. There is a different regime in place for data held by organisations operating in the telecommunications field. The Electronic Privacy Regulations (S.I. No. 535 of 2003 as amended by S.I. No. 526 of 2008) impose more specific obligations on telecommunications providers – including an obligation to inform subscribers of any "particular risk" of a breach of security. Substantial penalties can be imposed for breaches of these Regulations.

2.13. Revisions to the ePrivacy directive of December 2009 (2009/136/EC of 25/11/2009) will further develop this regime. The transposition deadline for the new provisions is 25 May 2011. The key points of relevance to the Group are:

- broad definition of "personal data breach";
- requirement to notify "such breaches to the competent national authority" (DPC in Ireland);

- requirement to notify such breaches to individuals where the breaches are "likely to adversely affect their personal data or privacy";
- requirement to notify individuals does not apply where technological measures (e.g. encryption) have been adopted "such as to render the data unintelligible to any person who is not authorised to access it";
- requirement to maintain a record of such breaches.

2.14. The revised Directive also requires the competent national authorities to have a range of oversight and penalty powers. (The DPC already has these powers in respect of the Telecommunications sector). The transposition deadline for the new provisions is 25 May 2011. The breach notification element is one small part of this Directive but is notable as an example of how the thinking at EU level is evolving.

Why Data Breaches Matter

2.15. Data breaches can damage an individual in different ways. Personal data that includes banking or credit card details can be used to defraud the individual. The unauthorised disclosure of personal information to third parties - especially if the information is of a sensitive or intimate nature - can be deeply distressing to an individual.

2.16. The possibility that disclosure to third parties may have taken place due to an inadvertent data breach can itself be a cause of distress. The measures that an organisation may advise its clients to take as a precaution against fraudulent misuse can also be inconvenient and costly to the clients. These factors might militate against notifying individuals where it is determined that a data breach is unlikely to lead to any negative consequences. Where even one unencrypted device containing personal data is stolen, this can give rise to significant concern about the damage and distress to the individual that could result from the misuse of this data, with a consequential degree of reputational (and potentially financial) damage to the organisation concerned.

Prevalence

2.17. Substantial data breaches have happened in Ireland. There is an increasing tendency to report them. Perhaps because of recent public concerns it is noticeable that there has been a significant increase in the use of encryption on devices such as laptops and USB keys. However, in the very recent past there have been cases of unencrypted data on stolen devices. Ireland does not seem to be outside the norm of countries for data loss and there is no evidence that this is a particularly Irish problem. By definition it is not possible to be exact about the numbers of breaches which have not been reported. A reasonable proxy may be those which have been brought to the attention of the Data Protection Commission by third parties. This would include instances where the organisation which has been breached, knew of

the breach but had not reported it or did not know before the data was discovered outside their organisation.

2.18. Data held by the DPC showed that, in 2008, there were 11 data breach cases where he was informed by third parties compared to 70 where the report came from the organisation. In these 11 cases the data controller said they were either unaware of the breach or unaware that they should notify affected data subjects. In all cases, where the issue was relevant, the DPC recommended that the subjects be informed and in all these cases the recommendation was complied with. (It would not be relevant where, for example the original notification first came from the data subject.) The equivalent figures for 2009 were 24 initially unreported breaches compared to 95 which were reported by the organisation themselves. Clearly, the number of breaches which are not reported to the DPC by third parties or by the organisations concerned is unknown.

2.19. Of the 86 organisations reporting breaches 60 were in the private sector and 26 were in the public sector. (The number of breaches does not equal the number of organisations because some organisations had more than one breach.) The four biggest categories of breach were: mailing issues (postal & electronic) 34; Theft/loss of equipment 27; Lost/stolen files 14 and website security issues 9.

2.20. Given

a) the quantities of data being held,
b) the growth in types and numbers of devices which hold significant quantities of data,
c) the degree to which individuals consent to handing over personal information and
d) the levels of general theft and computer related crimes,

it would be optimistic to assert that changing regulation on its own would eliminate such losses. However, better regulation can reduce the probability that these devices carry sensitive personal information in unencrypted, retrievable format. This would reduce the prospects of damage being done by such losses.

Some common points

2.21. There is substantial agreement on the financial and other damage caused by lost data. It seems clear that either the number of data breaches or the number of reported data breaches in many countries is increasing (or both). The Group shares the view that *prevention* of data loss by adhering to data protection principles is superior to incurring reputational and regulation costs following a breach.

2.22. There is a need to have a calibrated, balanced response as the regulatory element of reducing the probability of damage being done by lost data. Mandatory reporting of breaches to data subjects with penalties is in place in many States in the USA and is being actively considered by many other countries. It has recently been introduced in Germany and Austria.

2.23. The current DPC guidelines reflect the widespread recognition that individuals whose data has been lost or stolen need to be informed in a timely way where there is a significant danger that the breach may cause financial or other damage to the individual. Increasingly, common practical steps are being described on what should happen in cases of data breaches and how to go about reporting. The net issues are whether the taking of these steps should become mandatory and whether any penalties should apply.

2.24. There is increasing recognition that reporting breaches to regulatory authorities and/or data subjects is an important step in damage reduction. There are significant differences between countries in the underpinning regulatory structure to support breach reporting (legislation, guidelines, advice, best practice, codes of conduct). Because sensitive personal information is held by so many different types of organisation for so many purposes and in so many different forms there is a wide variety of national and international regulatory issues. While there are a number of specific standards, for example, ISO 17799/27001, there is no immediately identifiable single best-practice data security standard to which organisations can subscribe which covers all sectors. It would be expected that organisations which are certified to relevant ISO standards would have a low probability of data breach and a substantial defence against prosecution should a breach occur.

2.25. Guidance from the DPC on data security makes clear that an organisation which had achieved certification to such a standard would have demonstrated substantial compliance with the Data Protection Acts. Any organisation with such demonstrable commitment to best practice should therefore have reduced likelihood of breaches and, if breaches did happen, reduced prospect of prosecution. The practice of the DPC, where it currently has prosecution powers, is to use these powers sparingly to target repeat offenders or those who are reckless in relation to their data protection obligations. Prosecution is a matter of last resort and would be very rare. The prospect of prosecution with the ramifications for directors would be sufficient to improve concentration on the need for compliance. In the context of recent breaches, possibly only one of them would have resulted in a prosecution if the amendment now being proposed was available.

2.26. The recommendations of the Group are aimed at providing a proportionate solution to protect the rights of data subjects and give clear guidance to controllers of their responsibilities, to maximise compliance but provide a credible deterrent in line with emerging international practice to those who do not respect the rights of data subjects.

3. Review of existing legislative frameworks

3.1. The Group looked at its terms of reference under three main headings: Legal, Technical and Regulatory. The technical issues and regulatory *objectives* are broadly the same everywhere. However, the legal approaches and regulatory *frameworks* vary considerably from country to country. Appendix 4 itemises some relevant legal references.

EU/Council of Europe framework and recent developments.

3.2. The EU/Council of Europe model involves the setting of basic principles of data protection and providing rules for cross border flows of personal data. This model involves the establishment of an independent body to monitor the application of data protection law. The EU Directive on the protection of individuals with regard to the processing of personal data (Data Protection Directive)[1] is horizontal in its application. This means that it applies to any operation or set of operations which is performed upon personal data for the purpose of activities which come within the scope of EU law. The directive does not provide for mandatory reporting of data breaches. This Directive is complemented by the e-Privacy Directive. The Council of Europe data protection instruments[2] do not presently provide for mandatory reporting of data breaches.

3.3. Work has been intensifying at EU level to address the issues raised by mandatory reporting which are discussed in this document and in particular the differing EU legislative responses between data which is held in the context of telecommunications and other data. The data protection regime provided for in the Data Protection Directive has its origins at a time when data systems and telecommunications were fundamentally separate. There has, of course, been substantial technical and industry convergence in recent years. The revised ePrivacy directive seems to reflect current EU thinking. It seems likely that the breach reporting issue will harmonise towards the ePrivacy Directive level. Recital 59 of Directive 2009/136, referred to above, supports this view:

> "Pending a review to be carried out by the Commission of all relevant Community legislation in this field, the Commission, in consultation with the European Data Protection Supervisor, should take appropriate steps without delay to encourage the application throughout the Community of the principles embodied in the data breach notification rules contained in Directive 2002/58/EC (Directive on privacy and

[1] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

[2] Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data (Convention 108) and Additional Protocol to the Convention for the Protection of Individuals with regard to the automatic processing of Personal Data regarding supervisory authorities and transborder data flows.

electronic communications) regardless of the sector, or the type, of data concerned".

The elements of the Directive in respect of mandatory reporting are described at paragraph 2.13 above.

3.4. In respect of implementation and enforcement, the directive provides that Member States shall lay down rules on penalties, including criminal sanctions where appropriate, and shall take all measures necessary to ensure that the provisions of the amended Directive are implemented. The penalties should be effective, proportionate and dissuasive and may be applied to cover the period of any breach even where the breach has subsequently been rectified.

3.5. In addition, the Communications Regulator (Com Reg) – and where necessary other national bodies - will have the power to order the cessation of infringements. They will also have the necessary investigative powers and resources including the power to obtain any relevant information they might need to monitor and enforce the provisions of the Directive. They may also adopt measures to ensure effective cross-border cooperation when enforcing the laws.

3.6. As mentioned above, Member States have until the 25 May 2011 to transpose the Directive by adopting and publishing the laws, regulations and administrative procedures necessary to comply with the e-Privacy Directive.

Lisbon Treaty

3.7. The coming into effect of the Lisbon treaty has added a new institutional driver to the review of the existing Directive. Data protection has gained significant importance. Article 8 of the Charter of Fundamental Rights, which describes data protection as a fundamental right has become binding. Article 16 of the Treaty on the Functioning of the European Union was introduced as a new legal basis for data protection applicable to all processing of personal data, in the private and in the public sectors, including the processing in the area of police and judicial cooperation and common foreign and security policy – a new horizontal approach to data protection and privacy giving a foretaste of increasing harmonisation in this sphere.

3.8. The priorities for the EU Commission were laid out in the Stockholm Programme (June 2009) in their Communication “an Area of Freedom, Security and Justice serving the Citizen”. The priorities include:

- The Union must establish a comprehensive personal data protection scheme covering all areas of EU competence
- The Union must be a driving force behind the development and promotion of international standards for personal data protection.

3.9. In respect of the first goal, the Commission began a consultation on the legal framework for the fundamental right to the protection of personal data. This consultation closed at the end of 2009 and the results are under reflection by the EU Commission at present. It is understood that the preliminary position of the Commission is that the existing principles have stood the test of time but that more harmonisation and a new framework akin to that provided for in the ePrivacy directive may be needed. It is specifically committing to review mandatory breach reporting during 2010. The probability is that a new proposal will appear in late 2010 or in 2011. Commissioner Reding remarked during her confirmation hearing that *"fundamental rights and data protection will be top of the line"*. In October 2009 she had stated that *"It is absolutely essential that we find the right European responses to the concerns of European citizens about their fundamental rights to privacy and data protection. We cannot afford to lose their confidence in the information society if we want the potential benefits of the digital economy to become reality."*

3.10. In respect of the goal relating to the development and promotion of international standards, a High Level Contact Group between the US and EU, seeking to harmonise approaches and respect differences in legal bases and remedies, reported in November 2009. The overall objectives of this group are to promote the effective and safe transfer of data in the area of police and security cooperation between the US, EU and also third party countries.

3.11. All options likely to emerge from these activities include a high probability of mandatory breach reporting with substantial penalties. The issues around it include how to judge thresholds, responsibilities and penalties and the legal mechanisms to be put in place at national level to make these judgements. In some countries (e.g. UK and Spain) the regulator levies penalties. In other jurisdictions, including Ireland, judgements of this sort tend to be left to the judicial system. The existence of the potential for court action should help to improve the way in which organisations take care of the data they hold and at the margin dissuade some organisations from collecting or holding sensitive data at all.

3.12. In March 2008, the United Kingdom's Information Commissioner's Office (ICO) – the UK's data protection authority - issued a guidance note on data security breach management[3] and a further note specifically addressing notification of data security breaches to the ICO[4]. The notes advise that, though there is no legal obligation to report data security breaches, the Information Commissioner believes that serious breaches should be brought to the attention of his Office. The guidance note states that notification is not an end in itself but should have a clear purpose, whether to allow those affected to protect themselves or to allow regulatory bodies to perform their

[3] http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/guidance_on_data_security_breach_management.pdf

[4] http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/breach_reporting.pdf

functions, provide advice and deal with complaints. When deciding whether to notify the ICO, data controllers are encouraged to consider the potential harm to data subjects, the volume of personal data compromised and the sensitivity of the compromised data. The ICO decides whether to recommend that the data controller make the incident public based on their consideration of the public interest.

3.13. The UK's Data Protection Act was amended in 2008 to give the Commissioner the power to directly levy a monetary penalty on a data controller for serious breaches of data protection principles which were either deliberate or reckless. A consultation process on the level of penalty concluded recently and a maximum penalty of £500,000 has been prescribed which is due to come into effect in April 2010.

3.14. German Federal law, which came into force in September 2009, provides that data controllers, who believe they have lost data which puts their data subjects into "imminent risk", must report such losses simultaneously to the Data Protection Authorities (DPA) and directly to the data subjects. Substantial fines (up to €300,000) and other actions up to prohibiting the organisation from further processing are provided for. Austria introduced a mandatory breach reporting law at the end of 2009 with penalties for failure to report breaches.

3.15. The emerging consensus view within the EU would seem to be that breach reports should be made to Data Protection Authorities and in appropriate cases to data subjects. There is also some concern that a way of avoiding over-reporting and minimising bureaucratic overhead needs to be developed. As mentioned above, the new German legislation, which came into effect in September 2009, envisages a simultaneous report to the DPA and to the data subject.

3.16. Within this consensus there seem to be two broad approaches: one which looks at data breaches in the context of the general principles of data protection and another which looks more specifically at data breaches. The UK could be seen as an example of the former approach with Germany as an example of the latter

3.17. A Private Members Bill published by Fine Gael in 2008 envisaging breach reporting to the DPC in the first instance and then, in appropriate cases, within a short space of time to the data subject, adopts the latter approach.
http://www.oir.ie/viewdoc.asp?DocID=10087&&CatID=59&StartDate=01%20January%202008&OrderAscending=0

USA Framework

3.18. The mandatory reporting legislation in the USA forms part of a web of different approaches resulting in high levels of awareness of data breaches. There are different laws in different States. The US experience traces back to the passage of Californian breach reporting legislation in 2001, variations of

which have now been passed in more than 40 States. Thresholds, reporting formats and penalties vary from State to State - in some cases the breach is penalised in others failure to report is penalised. The various Acts are described in Federal Information Security and Data Breach Notification Laws **http://opencrs.com/document/RL34120/2009-01-29** .

3.19. It is not clear that the legislation has had the originally desired impact in terms of reducing the incidence of data loss. It may reduce the impact of losses by giving individuals the opportunity to mitigate harm. The number of recorded cases has continued to rise from year to year. This may be a function of the volumes of data being held and how it is being held, or that more breaches are now being disclosed because of the legislation. It may well be that there would be even more breaches than are currently being reported if the breach disclosure laws had not been passed.

3.20. The interactions under U.S. laws are, generally, directly between the data holders and data subjects, with data holders being obliged to inform data subjects of breaches if certain conditions are met. While the majority of laptop/usb/cd thefts and losses do not result in any direct harm, all notifications thereof cause some degree of individual apprehension and corporate reputational damage. There is limited case law on the topic – some class actions are at various stages in the U.S. Courts system seeking damages for harm done and also for apprehensions caused by notifications.

3.21. As the US, at both federal and state level, does not have the exact equivalent of EU Data Protection Authorities, reporting of data breaches to such authorities does not generally arise. However, agencies such as the Federal Trade Commission (FTC) perform many of the functions typically performed by a DPA, with very strong enforcement powers in cases where companies have failed to live up to their privacy promises to their consumers. (There are equivalent agencies in sectors such as health and financial services administration.) FTC action has resulted in the imposition of significant financial penalties on organisations that have been found guilty of data breaches.

Other frameworks

3.22. Australia, New Zealand and Canada have actively considered making disclosure of data breaches to Data Protection authorities mandatory but so far have not. In India and Malaysia, for example, legislation on hacking or theft is used to prosecute detected data protection offences including data breaches. In most countries there does not seem to be legislation in place to provide for the reporting of data breaches to data subjects. Large industry players such as Google, Accenture, Intel are also actively interested in harmonising the different international approaches to reduce business complexity and improve their compliance capacity. The Autumn 2009 International Conference of Data Protection and Privacy Commissioners approved a “Draft of International Standards on the protection of Privacy with regard to the processing of Personal Data” (Madrid Resolution). The draft

drew on existing standards developed by the EU, the Council of Europe, OECD and APEC (Asia Pacific countries).

3.23. Actions at international level to attempt to harmonise approaches to data protection reflect the fact that data flows around the world instantaneously. It can sometimes be difficult to establish exactly where all data held by internationally operating organisations is at any one time. It is probable that efforts will continue to internationally harmonise approaches to data protection, reflecting the importance of confidence in support of the free flowing of information on which modern economies depend.

Practical Legal issues in Ireland

3.24. A number of practical issues arise in the context of any proposed legislation. Unless the legislation provided for mandatory disclosure of all breaches, reporting requires a decision to be taken on whether the particular case merits reporting. There has been at least one case in Ireland where although the DPC had not felt a report of a breach directly to subjects was warranted, the organisation concerned chose to do so in the interests of transparency. An organisation may itself decide to report directly to the subject or seek a decision from the DPC on whether or not to report. This is a crucial decision with possible substantial financial and reputational consequences.

3.25. While the law is silent, in practice once a breach becomes known to the DPC, notification to the data subject, if relevant, has become standard once the DPC forms the view that the data subjects are open to the possibility of substantial damage or distress.

3.26. If reporting to Data Protection Commissioner was made mandatory this would leave the DPC to assess the impact on data subjects and to decide whether the data subjects needed to be notified. One example of the issues which would arise for determination would be if the Commissioner decided that notification was not necessary, how the right of data subjects to appeal against a decision of which they were not aware could be upheld. The application of the thresholds of substantial damage or distress arising from the breach and the test of whether the actions of the data controllers were reckless or knowing in the breach help address these questions but the answers would only come on a case by case basis.

3.27. A decision to report could have serious reputational and financial consequences even without administrative or court imposed fines arising. While a proportion of data losses certainly give rise to financial and other damage to individuals, many do not. But all notifications give rise to justifiable concerns. There is a view, based on the US experience, that there can be “notification fatigue” where there are frequent reports and the subjects do not notice any subsequent harm arising from the breach. Against this would be the view that it is the right of the subject to know and decide what action to take in respect of each loss of their data.

3.28. There is little case law or experience on the role of informed consent. People may have, by ticking a box to gain access to a service, allowed an organisation to harvest and share their details with third parties without really understanding the implications. They may consider that this constitutes a data breach if that organisation decides to use the data in some unforeseen way or if the privacy statement of the company was changed after they signed up to the service. There are, however, some indications from courts in the USA that the normal practice of an organisation relying on such an acceptance does not constitute a valid contract with the consumer as the company usually reserves the right to change the terms of the contract without prior consultation or notification afterwards. **http://www.theregister.co.uk/2009/04/23/blockbuster_lawsuit/**

3.29. From a regulatory perspective, it would seem appropriate that a more substantial penalty should be imposed on a careless organisation. In reality, the cost to the organisation of notification is likely to be a factor of the number of clients it needs to contact or offer remediation to as a result of the breach. The cost would be the same whether an organisation had been hacked or an employee had lost a laptop. Such costs can and do stretch to several hundred thousand euro. In the UK costs can arise from industry specific regulators concluding that a serious data breach is a general governance failure of an organisation and very big fines have been imposed (for example, the Financial Services Authority has fined HSBC £3m for failing to properly look after its customers' information and private data.) If small organisations or sole traders choose to collect personal data they must accept the stewardship consequences of this decision.

3.30. As mentioned previously, while there are individual industry standards, there is no universal security standard to which legislators or practitioners can point to determine whether an organisation had reasonable defences in place. The German legislation identifies the importance of encryption tools, but it can only specify that they be "state of the art" technology. Organisations which follow all relevant best practices may still experience a loss of their clients' data either through actions of individual employees or through malicious attack. The threshold of protection is changing all the time. There is often divergence of opinion on how serious a given threat is and it is difficult for even diligent practitioners to keep up with all the information that is flowing towards them and to discern which threats require most attention. In data security, as in other fields of endeavour, every problem has a solution. Every solution may also be the root of a new problem.

3.31. In the telecommunications area in Ireland, a very small number of prosecutions have been taken against a number of organisations, and specifically against their directors for whom the personal consequences of a conviction can be severe. These, it is understood, have proved to be very effective in improving the behaviours of not only the organisations which have been prosecuted but the industry generally.

3.32. The technology landscape is increasingly universal. Developments such as cloud computing, massive data centres, outsourcing, social

networking and small, high-capacity storage devices are everywhere a part of modern ICT-enabled economies. These developments are all contributing to increasing levels of flexibility, innovation and resourcefulness in organisations which embrace them. They also all contribute to difficulties in the organisations concerned meeting their obligations under the existing basic Data Protection principles. However organisations continue to have an onus to meet these obligations. They should also be aware of the reputational and financial losses that can follow lost confidence. Compliance with the principles will support their need to retain confidence in their custody of the clients' data. The principles which were derived in a technologically different era have, the Group believes, stood the test of time.

Civil Remedies for the Data Subjects

3.33. While the 1988 Data Protection Act creates a tort law duty of care this has not proved useful in practice. The defence of reliance on a third party and the fact that damage is virtually impossible to show in legal terms, make it unrealistic to expect the data subject to successfully police the data protection principles. This makes it all the more necessary for the State to provide meaningful criminal sanctions.

4. Technical issues

4.1. Technical issues are often thought of as being primarily the responsibility of specialists within an organisation. There can be a disconnect between people's desire not to get into technical issues and the degree of trust they demonstrate by using technology to hold their private, personal information. More and more private information is being given (or taken) on the understanding that it will be held safely. Data loss, while it has a technical aspect, is almost always a symptom of human lack of knowledge, carelessness or malice. Appendix 5 contains a set of indicative technical references.

4.2. Data protection legislation applies equally to data held on paper and data held by electronic means. This should continue to be the case. In addressing data loss, there is a necessary and significant focus on mobile storage devices such as laptops, USB keys and CDs lost by large organisations when the issue of data loss is discussed. The capacity of these devices to hold substantial amounts of personal data and the loss or theft of such devices from large organisations which has led to serious data breaches reinforces this. There are many other ways that data can be lost or stolen. Substantial data breaches have, for example, taken place via unshredded records discarded and found on dumps. The real question in most cases is how did sensitive data come to be on the lost device and why was it not protected?

4.3. The primary aim of action in this area should be seen as reducing the probability that information will find its way to people who should not have it. It was often stated in the early days of the widespread adoption of the Internet that "information wants to be free". Initially the "wild west" of the Internet was kept separate from tightly controlled corporate networks. Now they are closely intertwined. Technical developments operate to make it easier to carry and hold many more kinds of information in many more ways every year. Business trends reinforce the drive to do more with existing resources and to operate in many more locations. Breaking down barriers - "elimination of information silos" - is viewed as a good thing in the context of innovation; in the context of privacy and security it has a different connotation. Ease of use and security almost always operate against each other. Easy to use can often equal easy to lose.

4.4. Since the focus is on reducing the prospect of individuals being harmed by loss of sensitive personal data, the vast range of ways that data is held, and consequently can be lost, needs to be considered. Many evolving objects and techniques can be used for beneficial or malign purposes. The rapid changes in use and abuse of technology can challenge our capacity to define the concept of breach and lead to the view that legislation in the area of data protection should remain technology neutral. It follows that any legislation or regulations should be neutral on the format of notification – the appropriate method will vary from case to case.

4.5. The technical complexity and cost for organisations to hold data securely against hackers and web-based malice is increasing all the time. It can fall particularly heavily on small organisations with limited ICT expertise. Even large organisations can struggle to recruit and hold expertise. Loss from a small organisation can be just as harmful as that from large organisations. (Loss of medical records from a small surgery network could give rise to just as much harm as loss of records held by larger organisations.)

4.6. The drivers that exist to join up and examine data in new and fresh ways to gain competitive edge, to innovate or to provide better public service, for example, all challenge the principle that data collected should only be used for the purposes for which it had been collected. Decisions taken in good faith by organisations to repurpose or share data (shopping preferences, health information, anti-money laundering) could be interpreted as breaches of data subjects' rights. The substantive difference, from the subjects' perspective, would be that the breach arises from a conscious decision by a data holding organisation.

4.7. There are many examples where data is collected completely unknown to the data subject or known to them but where they may have no understanding of the uses to which it is being put. (e.g. material gathered from disadvantaged groups – as pointed out to the Group in the submission from Trust on behalf of homeless people). Organisations are also driven to join up the disparate data they have on individuals to give them an overview of their clients. Organisations may also need to gather, hold and share data for regulatory purposes. Further drivers to accumulate data are how easy it is to accumulate and how willing people are to hand it over. Within organisations chunks of organisational data can be broken off and used in (potentially malicious) ways unforeseen and without authority. As the Internet evolves towards the more collaborative Web 2.0 there is a further push towards removing boundaries and connecting previously unrelated holdings to give a "whole of customer" view and to work outside corporate boundaries. These behaviours are not particularly new, but the supporting technology is and there is certainly a powerful challenge to the successful protection of privacy. Information is easier to lose than to hold, easier to share than to keep private.

4.8. There are circumstances where a breach can occur despite the fact that the data controller has taken reasonable steps to protect it and may be unaware of the breach, either because the theft has been disguised, or because an individual working for an organisation has ignored or circumvented controls.

4.9. Large scale information holdings may pose qualitatively different challenges. Most commentary is focused on large organisations, public and private. In practice these organisations are likely to have substantial data protection policies in place. However, the massive expansion in personal data storage capacity poses challenges to individuals who may be unwittingly exposing their own, their family and colleagues' information to substantial risk of misplacement.

4.10. Issues arise where data is supplied by people who may not fully understand the implications of such mundane decisions as leaving cookies switched on or whose computers have been unwittingly infected (e.g. by a Trojan which copies any personal information it can locate). While much information exists on what is necessary to keep information on an ordinary Internet connected home computer private many people do not take the necessary steps to protect themselves. For example, a recent study based on an examination of a database of 32 million passwords which had been breached, showed the substantial majority of passwords in use to be easily guessed. (http://www.imperva.com/docs/WP_Consumer_Password_Worst_Practices.pdf) A separate survey showed that over 70% of people use their online banking passwords for a number of other unrelated non-secure sites. (http://www.trusteer.com/sites/default/files/cross-logins-advisory.pdf). Many technology-oriented websites and advice fora assume a level of interest that is higher than that demonstrated by most people. The well documented rise of "botnets" (where hundreds of thousands of computers have been hijacked and are controlled, unknown to their owners, by criminals) relies on people not managing the security levels of the computers they own. The purpose of these hijackings is primarily to take control of the infected computer and force it to deliver spam, harvest passwords or for targeted attacks. A side impact is that all the information on infected computers is compromised.

4.11. A further challenge arises from the changing face of personal information holdings. Previously unrelated pieces of name and address information, shopping habits, location information, CCTV images, age profiles are accumulated by third parties.

4.12. It is now accepted that passwords are of limited use as protective mechanisms and there is an increasing reliance on encryption for any sensitive information. While encryption is only as good as the care that is taken of the key, it is an essential requirement where personal data is being held on mobile devices of any sort. Unencrypted devices should not have sensitive data. This precaution is now so basic that it could form the basis for a symptomatic, risk-based enforcement approach - "being selective to be effective". Under existing Data Protection powers the DPC, in the course of their security audits, are confirming the encryption status of holdings of sensitive data held on mobile media as part of their assessment. It is accepted that the DPC's audit and investigative powers, including "dawn raid" capacity (which are stronger than those in, for example the UK) are being used well and are based on an assessment of organisations which are potentially at risk of holding sensitive personal information. The audits carried out include reviewing data security and encompass examining data holding devices. The impact of these audits would be greater if the outcome were immediately made public (clearly without any detail that would endanger an organisation's security) rather than being mentioned in the DPC Annual Report. For example, if a sample of an organisation's devices were audited and found to be unencrypted and carrying sensitive information then there would be a high probability that its other Data Protection practices would be found to be deficient. Having a demonstrable certification that their devices have been audited and found to be secure could well become a small but useful

competitive advantage as organisations deal with a client base increasingly worried about the potential harm from lost data.

5. Regulatory Issues

5.1. In its October 2009 Consultation Document the Group set out a range of indicative regulatory options. These are set out in Appendix 1. Appendix 6 has a range of regulatory references.

5.2. There is a wide variety of reporting experienced internationally. Some surveys have been done but it is questionable whether an organisation would publicly confirm that it has had a significant breach but never reported it. There are certainly mixed levels of awareness in organisations on their obligations under existing Irish legislation as illustrated in the submission by PricewaterhouseCoopers to the Group. Consequently there are varying levels of compliance.

5.3. There is no existing evidence of the role played by awareness of existing legislation where breaches have happened. Ignorance of the law would not be a defence in a specific case. But if it were demonstrated that there was a widespread pleading of ignorance as cases arose, then targeted information raising campaigns could be useful. A penalty-backed enforcement regime would be a fundamental change in the underlying principle of the existing law as it has been applied in Ireland to date (other than in the telecommunications area).

5.4. It is broadly in the interests of organisations holding data to hold it securely and not to allow breaches to happen. It may, however, also be in the interests of an organisation to share or exchange data with third parties and this can have unforeseen consequences. If penalties were to be introduced for data breaches arising from poor security and loss of data, it might seem to be an anomaly that there would not also be penalties introduced for cases where an organisation takes an active decision to release data contrary to the requirements of the data protection legislation and the data subject disagrees with that decision. This potential anomaly would be catered for by a more general provision which would include data breaches.

Regulatory Impact Assessment

5.5. The Group was asked to blend the needs of a Regulatory Impact Assessment with the work of the Group. All proposed legislation should now be informed by such an Assessment which is best done at the earliest stage.

5.6. There is a general role of regulation in forming part of a national reputation. A country perceived to be correctly regulated would be positively viewed externally. It is likely that the most recently developed regulatory regimes across a number of areas of activity would have common features. In this context, a breach reporting regulation (whether by law or otherwise) should be an example of the sort of regulatory regime in place in the country as opposed to being separate from other sorts of regulation in related areas of activity.

5.7. Any change in the regulatory regime will need to take account of the work of the High Level Group on Business Regulation led by the Department of Enterprise, Trade and Employment which is developing Risk Based enforcement policies to support the Government's strategy for economic recovery. Emerging policies include a consolidated inspections programme to reduce the number of inspection visits to business and a risk based assessment to minimise the burden on businesses. Protocols can be devised to minimise the overhead of audits on enterprises and on regulators' resources. The DPC already participate in a number of shared service initiatives.

5.8. An Impact Assessment of proposals to improve regulation on data breaches gives rise to a number of specific issues. These are discussed below.

5.9. **Need for regulation: evidence that the incidence of data breaches is increasing or reducing.** While there are many reports of data breaches (http://www.privacyrights.org/ar/ChronDataBreaches.htm) the meaning behind the reports is not immediately clear. It is possible that the incidence is static or reducing while the reporting proportion is increasing. However, the likelihood is that there are more breaches than previously and that there are more than are reported. It is not possible to say whether there are more breaches as a proportion of data being held. Although the report is drawn from the USA, the issues raised are likely to be more general. Consequently it seems that the existence of breach reporting legislation in the USA is raising awareness of the issue but not necessarily having the desired impact. It may be that there is a lag between the passage of legislation and its impact on organisations.

5.10. **Effectiveness of the current non-legislative reporting expectation.** The DPC has reported more organisations now choosing to report breaches to them as good practice and in their own interests. The DPC has power under existing legislation to issue Enforcement Notices and it is an offence not to comply. Where data breaches have come to the attention of the DPC, he has, where appropriate, raised the prospect of issuing an Enforcement Notice requiring that subjects be notified. In every case this has resulted in notification and the order has not had to be issued.

5.11. Therefore, where organisations have come forward to the DPC under existing guidelines there has been a subsequent notification to clients where the organisation and/or the DPC considered this to be justified. By definition, if organisations do not come forward, it is not possible to know for certain that a breach has occurred unless those unreported data losses subsequently become public because the data turns up. As mentioned before, a reasonable proxy for unreported breaches would be cases where no notification is made to the DPC before the data breach is discovered by third parties or media. Between 2008 and 2009 some 200 breaches of all sorts came directly or indirectly to the attention of the DPC with the substantial majority being reported by the organisations which had been breached.

5.12. Any proposals for a changed regulatory regime would need to be structured to encourage *early* reporting. The reaction of an organisation

which has discovered a breach and can approach the DPC with a view to establishing what needs to be done, including reporting to its customers may be different to the reaction of the same organisation faced with notifying the DPC and its customers and also a prosecution and substantial fine. By earliest reporting an organisation would show good intent at harm reduction and reduce the likelihood of prosecution.

5.13. **Determination of public interest.** An organisation might decide that they would run the risk of the lost data not turning up in any damaging way if the penalties for breaches were too high. However most organisations would, probably correctly, ultimately conclude that once they become aware of a loss of data it is unlikely that the matter will remain private and it is in their interests to report to the DPC and/or An Garda Síochána (if criminal activity is suspected) at the earliest stage. There may be a need for a more formal liaison between these two organisations on what steps to take where, for example, there is a view that notification might hinder a line of enquiry. A timely balance needs to be struck between the need for a successful apprehension of the culprits and the rights of potential victims to protect themselves.

5.14. Part of the rationale for not prosecuting or for reducing a penalty where an organisation has voluntarily reported a breach is because early notification gives an opportunity to pre-empt any financial harm. Stolen data can be used in a matter of hours and there may not be much time for a prolonged consideration of the matter if notification is to be of use.

5.15. Any proposed regulation would need to be calibrated to impose a greater cost on non-reported breaches which subsequently come to light to help organisations to balance the reputational damage of being found out (where organisations have lost data but haven't owned up) against the reluctance to self-incriminate.

5.16. **Equality of regulations between Public and Private Sectors.** It may broadly seem that there is a compulsion to give data to the Public Service but that giving data to private sector organisations is voluntary. Existing law does not distinguish between private and public sectors and it is unlikely that any revised regulatory arrangements could or should. While it is generally accepted that there is a higher onus on the Public Service this may derive from the fact that Public Service organisations tend to be monopoly suppliers. If individuals become discontent enough with a private sector supplier of a service they have the opportunity to change suppliers. Ultimately, regardless of sector, if senior (director level) individuals are held directly accountable for the safety of the sensitive data held by their enterprise the probability of the data being breached is lowered.

5.17. **Consequences of increased regulation in terms of cost of compliance.** The costs which may arise as a result of a breach (apart from reputational cost) include cost of notification, cost of indemnifying against damage done to clients, legal costs should civil actions or prosecutions ensue and cost of a fine if provided for in legislation. These costs would arise

directly to organisations should they cause or suffer a breach. Indirect costs would arise for taxpayers in any increased cost of administration and enforcement which would arise. Indirect costs might also arise if organisations enforcing a tighter information security regime tried to pass the cost on to clients. However the costs would be difficult to isolate and it would be difficult to justify a cost incurred for doing something the client is entitled to in any case – keeping personal information safe.

5.18. Regulation or legislation which would provide for mandatory disclosure, however it is brought in, would certainly add some cost to the activities of those who comply. Given the variety in scale and scope of data holdings and potential mechanisms for breach it is not possible to make calculations of costs of compliance with various options in a useful way. Organisations which are adhering to the Data Protection principle of holding data securely will, in any case, already be incurring a data security cost as a necessary part of doing their business, broadly equivalent to having an adequate insurance policy. Net direct additional costs arising from a mandatory reporting arrangement would only fall on organisations which are now holding data but have not appropriately secured it or which have breaches.

5.19. The cost of data loss prevention is likely to be the same in any economy. The cost of a data breach notification is also likely to be broadly the same. Given the emerging commonality of the requirement for breach notification (albeit under varying legal frameworks) there is little or no national advantage to be had in promoting a situation where the regulatory framework would allow for enterprises to minimise costs by saving on data security. There may be an intangible reputational loss if a state were considered to be under regulated by comparison with its peers in any particular sector. It is not thought that any proposals on how breaches are regulated, once they continue to be pragmatic, are likely to impact in a substantive way on location decisions. The elements under the control of the State are the costs of administering any regulatory infrastructure and the levels of any penalties. The former will be determined by the general policy of improving regulation and administrative retrenchment, the latter will be determined as legislation is drafted. The broad levels of penalty would need to be substantial, in line with those provided for in the ePrivacy Regulations, the German legislation or in the UK. The impact of such high penalties would be to reinforce the seriousness of the subject matter but also to reduce the likelihood of a large number of prosecutions.

5.20. The Data Protection Acts do not differentiate between large and small organisations in that their concern is to protect data. While there is an expectation that large organisations should incur the cost of tighter information security controls, smaller companies, clubs or individuals should also take risk-appropriate action. Once harm or apprehension of harm is conceived as a core issue, the relevance of who has released the data or how it was released are matters for consideration on a case by case basis. The introduction of a penalty, but at a low level, runs the risk of changing the existing relationship between organisations and the DPC, but being ignored in

the calculation on whether or not to disclose breaches. Much more substantial fines will certainly focus attention but would need to be proportionate to the severity of the breaches. The level of any penalty (which would be on foot of conviction for serious or repeated breach of any of the Data Protection principles) would effectively be set by the Courts but they would have levels available to them which would need to be in line with levels in other jurisdictions.

Laws, Policies and their implementation: Regulation in the real world.

5.21. It is comparatively straightforward to pass laws or state a high level policy that an organisation must not allow use of unencrypted data on devices such as USB drives. For an organisation to have an effective policy, it must put in place the capacity to enforce it. This includes ensuring that all concerned have the necessary understanding (legal, technical and practical) of what is needed to comply. Where they may be relying on third parties to support their IT, they need to ensure that their contractors also have a full understanding of the legal and reputational issues involved. Where companies do report breaches, it is clear that there is a variation in understanding within the organisations concerned of the technical issues or their capacity to address them. In cases where breaches have occurred, in Ireland or elsewhere, it is not clear whether, notwithstanding organisations' policy or training programmes, the people who have been primarily responsible have been aware of their obligations, or of the presence or absence of penalties.

5.22. A thorough data protection policy requires people to actively do some complex things as well as refrain from doing things which can seem harmless. A powerful behavioural change may be needed to bring this about. There may be a particular tendency to view a loss as something best kept quiet. The organisation and the individuals working for it need to comprehend that the full economic cost (direct financial costs, reputational costs including lost customers, potential fines, personal cost) of data loss is greater than the benefits to be derived from the perception that data is there to be mined and used to their individual and organisational advantage.

5.23. Fines and reputational damage at corporate level do not necessarily permeate the culture of an organisation unless consequences are seen to flow to responsible individuals. To reduce the prospect of harm being done needs an organisation, its employees and contractors to have a mainstream understanding of the issues. There is a continuing dichotomy between corporations wishing to centralise and control data and individuals wanting to use new tools to personalise their work experience.

5.24. Organisations, in particular, senior management, need to understand not only the importance of not losing their clients data but how to make sure that their employees and agents understand and carry out their obligations. In challenging times data security can be seen as a cost. To countervail this a cost needs to be introduced for illegally taking, improperly holding or carelessly losing data.

Communicating Risk

5.25. It is unlikely that legislation, regulation, statistics and risk analyses will change either corporate or individual behaviour on their own. To change behaviours it is necessary to change feelings rather than purely addressing the conscious mind (Slovic, Gazzaniga in "Risk, the Science and Politics of Fear" by Dan Gardner). Research is showing that people do not analyze risk in a conscious thoughtful way but analyse risk and benefit as if they were the relevant alternatives. (http://en.wikipedia.org/wiki/Affect_heuristic). In our current context both data holders and data subjects may well be underestimating the risks of providing data to be held as they have a general view of the good that comes from handing over the data. The growth in volumes of information being held is outside the scope of anything in history. It is difficult to get a comprehension of the quantities involved and for our internal risk assessment calculations to adjust accordingly.

5.26. It seems that there is a degree of disconnect between fears expressed about breaches and the day to day behaviour of handing over personal information to data holders. There is also some disconnect between organisations' statements of policy and practice on the ground. Regardless of the legislation and organisational protections being in place, breaches will happen. However, improved regulation can be shown to have reduced the incidence of, for example, cash in transit robberies and there is a fair expectation that this would be the result of improved regulation in the data protection area also. Improved regulation should be seen as a support to changing behaviour rather than a solution.

6. Conclusions and Recommendations

6.1. The Group examined a range of technical, legal and regulatory issues in relation to data breaches and the practices adopted in a number of countries. The Group also reviewed the emerging situation at EU level, in particular developments in the telecommunications sectors and the ePrivacy Directive, the impact of the Lisbon Treaty, the policy declarations of the new EU Commission and the development of the Commission's review of the Data Protection Directive. The timing of any legislation would, likely be influenced by the quickening pace of these developments – predominantly those under consideration by the EU Commission. It is now probable that the review of the existing Data Protection Directive will give rise to a proposal for a new or amending Directive either later this year or during 2011. The indications are that this new proposal will address many of the issues covered by the work of the Group, in particular providing for some form of mandatory notification to data subjects in cases of data breach. The Group took note of the enhanced competence available to the Commission in this area following the coming in to force of the Lisbon Treaty.

6.2. A range of regulatory options were identified and these were set out in the public Consultation Paper issued by the Group in Autumn 2009 to elicit views and concerns of interested parties. The range of options is included at Appendix 1.

6.3. The Group did not consider that a self-regulating regime (even if externally audited), where organisations would be left to decide for themselves whether or not to report data breaches, was desirable or practical.

6.4. The Group, having considered the matter in some detail, concluded that data breaches are symptomatic of breaches of the broad principles of Data Protection. It was the view that these principles, in themselves, continue to work well. The Group noted that none of the data protection principles is afforded primacy in data protection law. In addition, the Group noted that reporting of data breaches is not, of itself, one of the principles but can be important in assessing potential damage caused by breaches of the security principle.

6.5. In examining the issues surrounding breach reporting the Group drew a distinction between reporting to the DPC and reporting to individuals affected by the breach. While the Group concluded that there should be a requirement for breach reporting to the DPC it did not feel compelled to recommend the creation of a direct legal requirement to report breaches to individuals concerned. The decision to report breaches to affected individuals is, in the first place, a matter for consideration by the data controller and, secondly, for the DPC. The Group concluded that the requirement to report breaches to individuals was best moderated through reporting to the DPC.

6.6. In examining the most effective legislative changes the Group considered two options viz,

- specific legislation for data breach reporting in a narrow context, or
- more general legislation taking the wider issues into consideration.

The Group wanted to ensure that, in making any recommendations about breach reporting they address the underlying causes of data breaches which give rise to the need for reporting. Accordingly, they opted for the more general approach to the issue by proposing an offence relating to the contravention of the data protection principles.

6.7. It is the view of the Group that the DPC already has adequate powers to require that organisations inform individuals of a data breach affecting them. The DPC can, if necessary, issue an Enforcement Notice and failure to comply with such a Notice is an offence. However, the DPC can only act in such cases when he becomes aware of a data breach.

6.8. The Group recommends that a statutory Code of Practice, based on the existing DPC guidelines, be introduced and proposes that it would be an offence not to comply with this Code. The Code would, inter alia, set out the circumstances in which reporting to the DPC would be obligatory. The Group concluded that data breaches can be a symptom of a culpable failure to comply with general data protection principles, especially in relation to data security. The Group, therefore, recommends the creation of a separate offence relating to deliberate or reckless acts or omissions in relation to the data protection principles. The Group recognises that the introduction of such an offence would amount to a fundamental change to the existing legislation and some reservations were expressed about this.

6.9. The Group does not suggest any changes to the current arrangements for the imposition of penalties or sanctions under the Data Protection Acts. Given the range of potential methods of breaching, the range of case by case decisions needing to be taken by the data controlling organisation and the DPC, and the range of defences which could be mounted, the Group is of the view that the Courts are best placed to hear individual cases and make determinations.

6.10. The Group considered that any measures taken should be technology neutral insofar as possible and that timely revisions of the relevant Code of Practice should be undertaken to ensure that law keeps pace with technological innovation.

Recommendations

6.11. The Group recommends that:

1. Legislation should provide for a general offence by a data controller of deliberate or reckless acts or omissions in

relation to the data protection principles – including contraventions of the security principle in relation to data breach incidents. This would complement the existing offence under the Data Protection Acts for failure to comply with an Enforcement Notice issued by the DPC - including an Enforcement Notice directing a data controller to inform individuals of a data breach affecting them.

2. The reporting obligations of data controllers in relation to data breaches should be set out in a statutory Code of Practice as provided for under the Data Protection Acts. The Code, broadly based on the current guidelines from the DPC, should set out the circumstances in which disclosure of data breaches is mandatory. Failure to comply with the disclosure obligations of the Code could lead to prosecution by the DPC

3. The Code should be reviewed on a regular basis by the DPC and amendments submitted to the Minister as necessary to keep the legislation current.

4. The DPC should continue to develop his investigation and audit activities in a targeted way, with a particular focus on organisations which hold sensitive personal data, in compliance with emerging risk-based approaches to enforcement.

5. Legislation should provide for the timely publication of the outcome of such DPC audits, as an aid to good practice and in the interests of transparency.

6. The DPC should continue to develop public awareness activities in this area.

Appendix 1

Table of regulatory options included in Data Protection Review Group's Consultation Paper

Regulatory Option	Pro	Con
1. No further development of the existing DPC Guidelines pending new EU directive.	De facto many organisations who lose data are now contacting DPC/Gardaí No recent example of organisation advised by DPC to report loss to customers refusing to do so Organisations making reports incur costs which are directly related to the scale of their breach Does not add any new regulatory burden Allows for emergence of EU level directive and avoids double legislation Keeps existing encouragement, educative approach	Reporting is not mandatory and has no statutory basis In principle, breaches of duty should attract penalty EU directive may not emerge in timely fashion
2. Further Develop Code of Conduct and awareness campaign under existing legislation (e.g. commission risk based audit of organisations' devices and publish results; increased levels of information on costs of data loss, develop guidance on thresholds)	Keeps focus on fundamental Data Protection principles rather than on specifics Treats visible symptom (lost data) as indicator of underlying poor practice Increase awareness of existing legislation Limited additional regulation cost Flexible and in line with emerging National regulatory approach – serious breaches could, in risk based evaluation flag up attention of other regulatory bodies Allows for emergence of EU level directive and avoids double legislation	Focussing on only one symptom Does not introduce penalties for offenders No specific penalty apart from reputational cost to organisation of failing an audit and cost of subsequent more detailed audit Additional cost of increased audit activity may need to be offset by reduced activity in other areas. Cost of awareness raising activities

3. Legislate for penalties for very serious contraventions of the Data Protection Acts, with failure to report significant data breaches to the DPC and to data subjects being considered as aggravating factors in a contravention of the data security provisions of the Acts	Model being implemented in the UK, following consideration of different options Keeps the focus on overall compliance with the DPA rather than focusing on only one aspect Responds to a more general demand that serious contraventions of the DPA should attract penalties and that failure to have such penalties can lead to a relative neglect of data protection within an organization Would encourage DPC to only use penalty powers for the most serious breaches Would eliminate the anomaly of penalties for relatively minor breaches of the ePrivacy Regulations but no penalties for even the most serious breaches of the DPA	Penalty provisions could encourage a less cooperative approach between data controllers and the DPC Danger that DPC could be pressurised into using penalty provisions in inappropriate cases e.g. in response to manufactured media outrage Relies on organisations to decide on reporting thresholds More legal costs
4. Legislate for mandatory reporting to DPC for data breaches with penalties for serious breaches or failure to report or both. DPC decides on whether and how to notify	Would introduce penalties into Data Protection legislation and improve levels of protection Place stronger onus on data holders controllers to comply with Data Protection Principles Would improve general levels of data security Would cover all potential breaches equally – without threshold every incident would call for a report. DPC role would allow for consistency of decision making and help avoid over reporting to data subjects	Changes legislation from cooperative, educative to penalising. Difficult to have penalties for one aspect of data protection failure but not for any other. Introduces additional business cost (but only for those who breach – the cost of any penalty.) Potential for over reporting if people are in receipt of multiple notifications Penalties would require prosecutions where convictions may be difficult to secure unless a system of administrative

	Provides more direct legislative support for DPC guidelines	penalties imposed by the DPC were introduced. May not be in line with new EU directive Could overwhelm resources of DPC and result in reduced timeliness of notification to data subjects
5. Legislate for mandatory reporting to DPC above defined threshold with penalties for serious breaches or failure to report or both	As for 4 but would focus on large scale breaches, either in terms of numbers of records, severity of breach or range of information lost, Reduce danger of over reporting and associated report fatigue Legislative support for existing ad hoc arrangement where organisations are increasingly approaching the DPC and being advised to notify data subjects.	As for 4. Objective threshold difficult to establish. Judgement and complex decision required in a very short space of time Additional resources needed for DPC to allow timely discharge of function
6. Mandatory simultaneous reporting to DPC and to data subjects all breaches.	As for 4. Eliminates any time delay in DPC reaching a decision to report or not report and improves chance of data subject to effectively take precautions. Affirms primary relationship is between data subject and data holder. Leaves the client the choice of how to react. DPC can subsequently follow through seeking penalties for breach	As for 4. "Crying wolf" danger of over reporting Potentially heavy cost on business disproportionate to businesses operating in other EU jurisdictions Primary decision on what constitutes a breach remains with data controller
7. Mandatory simultaneous notification to DPC and to data subjects all breaches above threshold	As for 5. Helps reduce over reporting if threshold is consistently defined and applied Guidance could be given from DPC on how thresholds would apply.	Difficulty of defining objective threshold. Introduces a potential delay while organisation considers whether notification is necessary

	Organisations could rely on having complied with these guidelines if challenged. Follows new German model	
8. Mandatory reporting directly to data subjects all breaches, penalties for failure to report	Most closely follow US model Affirms primacy of data subject's role Low administrative cost for the state Organisations may be tempted to weigh likely penalty against known cost of report	Danger of over reporting Reduces educative, guidance role of DPC Moves away from current EU mainstream Relies on organisations alone to decide on thresholds More legal costs

Appendix 2

Submissions Received by the Data Protection Review Group

BH Consulting

Digital Rights Ireland

Global Privacy Alliance

Irish Banking Federation

Irish Computer Society - Security Professionals Network

Mr Sam Johnston, Certified Information Systems Security Professional

Mr David Nolan

PricewaterhouseCoopers

Trust Ireland.

4 submissions from persons raising individual points.

Appendix 3

Indicative Data Breach Incidents and responses. This is not a comprehensive listing . Organisations are mentioned insofar as they have been referenced in the public domain.

1.US website itemising a chronology of Data Breaches the data breaches noted below have been reported because the personal information compromised includes data elements useful to identity thieves, such as Social Security numbers, account numbers, and driver's license numbers. Some breaches that do NOT expose such sensitive information have been included in order to underscore the variety and frequency of data breaches.... it is not a complete listing of breaches. The list is a useful indication of the types of breaches that occur, the categories of entities that experience breaches, and the size of such breaches. But the list is not a comprehensive listing. Most of the information is derived from the Open Security Foundation list-serve (see below) which is in turn derived from verifiable media stories, government web sites/pages, or blog posts with information pertinent to the breach in question. Many breaches (particularly smaller ones) may not be reported. If a breached entity has failed to notify its customers or a government agency of a breach, then it is unlikely to be reported anywhere. http://www.privacyrights.org/ar/ChronDataBreaches.htm

Sample one month extract from January 09 records in the Chronology. It contains a representative mix of breaches showing a variety of methods and scale. The instances are in the order in which they appear in the report and date references are from January 2009

> **"Merrill Lynch**. A third-party consulting services firm working on behalf of Merrill Lynch reported, one of their employees was burglarized. The burglars took various items, including a computer, which had on it the names and Social Security numbers of current and former Financial Advisors and some applicants for employment.
>
> **Pepsi Bottling Group** a portable data storage device, which contained personal information, including the names and Social Security numbers of employees in the US is missing or stolen.
>
> **Library of Congress** (Washington, DC) An employee in the human resources department of the Library of Congress was charged with conspiring to commit wire fraud in which he stole information on at least 10 employees from library databases. He passed the information to a relative, who used it to open the accounts. Together, the two are alleged to have bought $38,000 worth of goods through the accounts.
>
> **CheckFree Corp**.(Atlanta, GA) CheckFree Corp. and some of the banks that use its electronic bill payment service say that criminals took control of several of the company's Internet domains and redirected customer traffic to a malicious Web site hosted in the Ukraine. The company believes that about 160,000 consumers were exposed to the Ukrainian attack site. However, because the company lost control of its Web domains, it doesn't know exactly who was hit. And so it must warn a much larger number of customers. This breach was reported back in Dec. 3 08. 5,000,000 records.

Genica/Geeks.com (Oceanside, CA) recently discovered that customer information, including Visa credit card information, may have been compromised. In particular, it is possible that an unauthorized person may be in possession of your names, addresses, telephone numbers, email addresses, credit card numbers, expiration dates, and card verification numbers. They are still investigating the details of this incident, but it appears that an unauthorized individual may have accessed this information by hacking our eCommerce website.

University of Rochester (Rochester, NY) Personal information including Social Security numbers of about 450 current and former University of Rochester students was stolen by hackers this week from a UR database. The information was taken from a non-academic student database and copied illegally to an off-campus IP address. 450 records

Columbus City Schools (Columbus, OH) Columbus City Schools experienced a security breach, resulting in employees' Social Security numbers being at risk. CPD officers went to serve drug and auto-theft felony warrants. During the arrest officers learned there might be stolen personal information in the house and found personal information on district employees. It is believed the suspects either stole or intercepted part of a mailing from the payroll division that was en route to annuity companies. 100 records.

University of Oregon A laptop computer containing data files for Youth Transition Program (YTP) participants was stolen. Those files contained names and social security numbers.

Innodata Isogen, Inc. Laptop stolen from an employee's car contained names, addresses, Social Security numbers of current and former employees.

Seventh-Day Adventist Church A Laptop stolen and recovered contained names and Social Security numbers. 292 records

Continental Airlines A laptop containing fingerprints, Social Security numbers, names, addresses, was stolen from a locked Newark office. 230 records

Blue Ridge Community Action Social Security numbers were on an external computer hard drive that is missing or stolen. The hard drive contained information on clients from four counties who have used the organization's services in the past four or five years. The external hard drive was used to back up information on clients. 300 records

Occidental Petroleum Corporation A former employee emails himself (to personal email account)a spreadsheet of employee names, addresses, employee identification numbers, birth dates, starting dates, retirement dates and Social Security numbers. **Southwestern Oregon Community College** A laptop computer was stolen from the campus putting former and current students at risk. 200 records.

Forcht Bank Customer debit cards were disabled this week after learning they could have potentially been hacked into by persons creating duplicate cards. The cards were comprised when a retail merchant's computer system was hacked. Which merchant is unknown at this time. The breach affected customers of multiple banks and multiple debit and ATM networks. 8,500 records

Kanawha-Charleston Health Department(Charleston, WV) People who received flu shots from the agency since October, are being warned that their

personal information may have been stolen by a former department temporary worker. Information included their names, social security numbers, addresses and other personal information. 11,000 records

Heartland Payment Systems After being alerted by Visa and MasterCard of suspicious activity surrounding processed card transactions, the company last week found evidence of malicious software that compromised card data that crossed Heartland's network. This incident may be the result of a global cyber fraud operation. **UPDATE** (1/26/09): Heartland Payment Systems has been sued. The lawsuit seeks damages and relief for the "inexplicable delay, questionable timing, and inaccuracies concerning the disclosures" with regard to the data breach, which is believed to be the largest in U.S. history. **UPDATE** (2/12/09): According to BankInfoSecurity.com, the number of financial institutions that have come forward to say they have been contacted by their credit card companies Visa and MasterCard in relation to the breach has jumped from fewer than 50 to more than 200. **UPDATE** (6/4/09): While it's hard to get a handle on just how many consumers were affected by the Heartland Payment Systems (HPY) data breach, the total number of institutions now reporting card compromises is at 656. **UPDATE** (6/16/09): Heartland Lawsuits to be Heard in Texas. The Judicial Panel on Multidistrict Litigation in Louisville, KY issued its decision to consolidate the class action suits. The lawsuits will be heard in the Southern District Court of Texas in Houston. Thirty-one separate lawsuits, on behalf of consumers, investors, banks and credit unions, have been filed against Princeton, N.J.-based Heartland. **UPDATE** (7/6/09): Heartland Payment Systems completed the first phase of an end-to-end encryption pilot project designed to enhance security. It is unclear how many account numbers have been compromised, and how many are represented by multiple transactions. The number of records breached is an estimate, subject to revision. Heartland deals with 100 million transactions per month

First Interstate Mortgage Corporation (FIM)/Nevada One Corporation (Nevada One) These mortgage brokers have been discarding consumers' tax returns, credit reports, and other sensitive personal and financial information in an unsecured dumpster. Approximately 40 boxes containing consumer records were found in a publicly-accessible dumpster. The records included tax returns, mortgage applications, bank statements, photocopies of credit cards, drivers' licenses, and at least 230 credit reports. The defendant, who has owned numerous companies that handle sensitive consumer information, kept the documents in an insecure manner in his garage

Missouri State University Personal information, including Social Security numbers for 565 foreign students at MSU was leaked this month when a university office sent an e-mail message soliciting their help with language tutoring. The email message they got had a spreadsheet attachment that contained names and Social Security numbers for international students. 565 records

Monster.com Their database had been illegally accessed and user IDs, passwords, names, e-mail addresses, birth dates, gender, ethnicity, and in some cases, users' states of residence were stolen.

Madison, WI. Human Resources Department An oversight by the city of Madison's personnel office is the reason Social Security numbers of city employees were stored on a laptop computer stolen from a city office. Any

official or employee — except those in the police, fire and transit departments — who was issued a new or replacement city identification card from the start of 2004 through 2007 may be at risk. Data on the laptop included photos, names and Social Security numbers. 500 records

U.S. Military A New Zealand man accesses US military secrets on an MP3 player he bought from an Oklahoma thrift shop for $18. When the 29-year-old hooked up the player he discovered a play list he could never have imagined - 60 files in total, including the names and personal details of American soldiers.

U.S. Consulate Hundreds of files — with Social Security numbers, bank account numbers and other sensitive U.S. government information — were found in a filing cabinet purchased from the U.S. consulate in Jerusalem through a local auction. 2009 **Beaumont City** Personal information of current and former Beaumont city workers was accidentally posted online. The information, including birth dates and Social Security numbers. 500 records.

Citi Habitat During a refurbishing of their office, paper that should have been shredded was improperly placed as trash. Information found blowing in the street included bank statements, 401k statements, credit reports, tax returns, driver's licenses, names, phone numbers and Social Security numbers.

CityStage (Springfield, MA) A computer system might have exposed credit card information of customers on the Internet. It probably occurred in December while the theater's Web contractor was changing servers. Credit card numbers might have been compromised.

Kansas State University Students who were enrolled in an agricultural economics class in spring 2001 inadvertently had some personal information exposed on the Internet through a K-State departmental Web site. Names, Social Security numbers and grades of those students have been exposed since 2001. 45 records

Coos Bay Department of Human Services A scammer made off with Social Security numbers after sending a virus online to a computer at the Department of Human Services office. A application that was installed recorded keystrokes and sent them to an external address. The information was taken from Coos County residents. **Indiana Department of Administration** Social Security numbers of current and former state employees were accidentally posted on a state Web site for about two hours. The Social Security numbers were erroneously included in a contract solicitation file posted on the department's procurement Web site. 8,775 records

HoneyBaked Ham A computer server stocked with credit-card information was stolen from a store. Customers might be at risk

Ball State University A employee sent out an e-mail, to verify contact information, to 91 special events staff with an excel spreadsheet attachment that, unbeknownst to the employee, included the Social Security number of 19 of the workers. **”**

The above extract from January 2009 is representative of any recent month in the chronology.

2. DataLossDB is a research project aimed at documenting known and reported data loss incidents world-wide The Open Security Foundation, as well as our volunteers, feel that there is a distinct need for tools that provide unbiased, high quality data regarding data loss. **http://datalossdb.org/about**

3. A laptop containing private details, including bank details, of 30,000 civil servants across Northern Ireland was stolen during a break-in at a government office in Belfast. **http://www.siliconrepublic.com/news/article/13113/cio/30-000-civil-servants-details-on-stolen-laptop**

4. French government probing Sarkozy bank theft(AFP) – Oct 19, 2008 PARIS (AFP) — The French government has launched a probe into withdrawals by thieves from President Nicolas Sarkozy's personal bank account, said a senior official Sunday. **http://afp.google.com/article/ALeqM5hwrR93MpSzps2leIcVs0arWmiyjg**

5. The computer systems of both the Obama and McCain campaigns were victims of a sophisticated cyber attack by an unknown "foreign entity," prompting a federal investigation, NEWSWEEK reports today……both the FBI and the Secret Service came to the campaign with an ominous warning: "You have a problem way bigger than what you understand," an agent told Obama's team. "You have been compromised, and a serious amount of files have been loaded off your system." **http://www.newsweek.com/id/167581**

6. Irish Independent February 08 2008 "HACKERS are targeting state departments for sensitive information. More than 80 government laptops have been stolen or are missing, raising fears about the protection of confidential data. The Irish Independent has learned the laptops and computers have been lost or stolen over the past five years, triggering concerns sensitive information may be vulnerable. Four government-controlled websites were also recently the victim of cyber-attacks and telephone hacking incidents. A garda investigation is under way in the Department of Enterprise, Trade and Employment, which experienced four "noteworthy hacking or cyber-attacks". The Department of Transport was the subject of a "malicious security breach" and is blocking an average of 50 inappropriate attempts to connect to its systems every week.....The incidents also include the loss or theft of 19 Blackberrys and 10 memory keys. In the Department of Social and Family Affairs -- which has responsibility for social welfare payments -- five laptops were stolen on public transport and in house and car break-ins. According to the Department of Defence, two desktop computers belonging to the Defence Forces were stolen last year ..Last year, 12 laptops belonging to the Department of the Environment were stolen from the Custom House and another was stolen while in transit. Ten were immediately recovered, nine of which were obsolete and had been prepared for recycling. The three laptops missing from the Taoiseach's office did not contain sensitive State information, a spokesman said last night. Last night, a leading expert on data protection law said the more public servants who can access the data, the more likely something will go wrong. Professor Robert Clark of UCD said "human error" can account for most data breaches. " **http://www.independent.ie/national-news/fears-for-our-personal-data-as-80-government-laptops-missing-1284944.html**

7. Article from " The Banker" re data breaches with special reference to banks **http://www.thebanker.com/news/fullstory.php/aid/5930/Plugging_the_leak.html**

8. A contractor to the Home Office, PA Consulting, lost an unencrypted memory stick containing the sensitive personal information of thousands of people last year. The ICO has now made the Home Office sign a formal undertaking to protect citizens' data. **http://www.out-law.com/page-9731**

9. The new head of MI6 has been left exposed by a major personal security breach after his wife published intimate photographs and family details on the Facebook website. Sir John Sawers is due to take over as chief of the Secret Intelligence Service in November, putting him in charge of all Britain's spying operations abroad. **http://www.mailonsunday.co.uk/news/article-1197562/MI6-chief-blows-cover-wifes-Facebook-account-reveals-family-holidays-showbiz-friends-links-David-Irving.html**

10. Almost two million PCs globally, including machines inside UK and US government departments, have been taken over by malicious hackers. Security experts Finjan traced the giant network of remotely-controlled PCs, back to a gang of cyber criminals in Ukraine **http://news.bbc.co.uk/2/hi/technology/8010729.stm**

11. The details of bank accounts held by 21 million Germans are for sale on the black market for 12 million euros (15 million dollars), a German magazine reported Saturday. In an investigative report, two reporters for the Wirtschaftswoche magazine met last month with two individuals, arranged through an intermediary, who offered to sell a CD-ROM containing the names, addresses, bank name and account numbers of 21 million people. **http://www.breitbart.com/article.php?id=081206224148.ie9uiizl**

12. Detailed and sensitive bank information of tens of thousands of German credit card customers have been stolen in what investigators have described as the worst ever case of data theft in the country **http://www.thelocal.de/national/20081213-16107.html**

13. Employees routinely engage in activities that put sensitive data at risk. They are downloading data onto unsecured mobile devices (61%), sharing passwords (47%), losing data-bearing devices (43%), and turning off their mobile devices' security tools (21%). And, reflective of the blurring of the lines between personal and professional lives, they are using web-based personal email in the office (52%), downloading Internet software onto an employer's devices (53%), and engaging in online social networking while in the workplace (31%). **http://www.ponemon.org/blog/post/more-employees-ignoring-data-security-policies**

14. Verizon Business 2009 Data Breach Study Finds Significant Rise in Targeted Attacks, Organized Crime Involvement. *Financial Industry Accounts for 93 Percent of 285 Million Compromised Records; Most Breaches Avoidable if Proper Precautions Taken* More electronic records were breached in 2008 than the previous four years combined, fuelled by a targeting of the financial services industry and a strong involvement of organized crime…… nearly nine out of 10 breaches were considered avoidable if security basics had been followed. Most of the breaches investigated did not require difficult or expensive preventive controls The 2009 report concluded that mistakes and oversight failures hindered security efforts more than a lack of resources at the time of the breach. Similar to the first study's findings, the latest study found that highly sophisticated attacks account for only 17 percent of breaches. However, these relatively few cases accounted for 95 percent of the total records breached - proving that motivated hackers know where and what to target. http://newscenter.verizon.com/press-releases/verizon/2009/verizon-business-2009-data.html

15. Fourth annual *U.S. Cost of a Data Breach Study*. According to the study which examined 43 organizations across 17 different industry sectors, data breach incidents cost U.S. companies $202 per compromised customer record in 2008, compared to $197 in 2007. Within that number, the largest increase in 2008 concerns lost business

created by abnormal turnover of customers. Since the study's inception in 2005, this cost component has grown by more than $64 on a per victim basis, nearly a 40% increase.
http://www.pgp.com/insight/newsroom/press_releases/2008_annual_study_cost_of_data_breach

16. Over a third of IT staff use their administrator rights to have a peek at confidential company information, including customer databases and HR lists, according to a recent survey carried out by security software firm Cyber-Ark on 400 senior IT professionals in mainly enterprise-class firms across the UK and US. **http://www.siliconrepublic.com/news/article/13156/cio/35pc-of-it-staff-admit-to-snooping**

17. "Acerno, which has operated for three years with almost no publicity, says it now has files on 140 million people in the United States, nearly all the online shoppers…. Unlike in Europe, where data collection is closely regulated, in the United States, the privacy framework is based on what is called "notice and choice." In other words, it's fine to gather and use information so long as you tell people what you are doing so and give the option to make you stop. On the Internet, however, the way this has worked is based on a complete fallacy: that Web site users read the privacy policy. Here is the bluntest way to put the question: Is a notice really a notice if the vast majority of people who are supposed to be notified don't notice the notice? " **http://bits.blogs.nytimes.com/2008/10/24/what-online-stores-sell-data-about-you/**

18. "Fewer than half of UK companies use encryption technology to secure their data. Despite the lack of encryption, UK IT managers claim their corporate data is safe and almost two-thirds (65 per cent) said the HM Revenue & Customs (HMRC) data breach will not change their IT spending priorities, according to a survey by Check Point" . **http://management.silicon.com/itdirector/0,39024673,39169337,00.htm**

19. "Veterans Sue [Veterans' Administration] VA over Data Loss. The lawsuit, which comes days after the VA reported that the personal information of 26.5 million veterans was stolen from an employees home, seeks damages of $1,000 for every person listed in the missing database files. The suit also asks that the courts prohibit the VA from handling any personal privacy-protected data except under court supervision, and that the court create a set of "consensus minimal security standards" under which the VA can operate" **.** **http://www.eweek.com/c/a/Security/Veterans-Sue-VA-over-Data-Loss/**

---

20. "The German government says it plans to buy a CD containing customer data apparently stolen from British bank HSBC's operation in Switzerland. The move has enraged Swiss officials, but it already appears to be bearing fruit. Berlin expects a wave of tax evaders to turn themselves in over the coming days in the hope of avoiding prosecution " **http://www.spiegel.de/international/germany/0,1518,675723,00.html**

21. "Online banking fraud involving the electronic transfer of funds has been on the rise since 2007 and rose to over US$120 million in the third quarter of 2009, according to estimates presented Friday at the RSA Conference in San Francisco, by David Nelson, an examination specialist with the FDIC.[Federal Deposit Insurance Corporation]

The FDIC receives a variety of confidential reports from financial institutions, which allow it to generate the estimates, Nelson said.

Almost all of the incidents reported to the FDIC "related to malware on online banking customers' PCs," he said. Typically a victim is tricked into visiting a malicious Web site or downloading a Trojan horse program that gives hackers access to their banking passwords. Money is then transferred out of the account using the Automated Clearing House (ACH) system that banks use to process payments between institutions.

Even though banks now force customers to use several forms of authentication, hackers are still stealing money. "Online banking customers are getting too reliant on authentication and on practicing layers of controls," Nelson said"

http://www.pcworld.com/article/191019/fdic_hackers_took_more_than_120m_in_three_months.html

22. "US healthcare corporation Health Net kept quiet for 6 months about a lost disk drive, exposing 1.5 million of its members to identity theft. It is now being sued. The law suit, filed by Connecticut's Attorney General, Richard Blumenthal, is in regard of 466,000 members in that state and refers to HIPAA regulations." **http://vawatchdog.com/10/nf10/nfjan10/nf012010-1.htm**

23. "A school district in Pennsylvania spied on students through web cameras installed on laptops provided by the district, according to a class action lawsuit filed this week" **http://www.guardian.co.uk/world/2010/feb/19/schools-spied-on-students-webcams**

24. "About 75,000 personal computers in almost 2,500 companies and government agencies worldwide have been caught in a botnet based on a new variant of the ZeuS Trojan".**http://www.guardian.co.uk/technology/2010/feb/18/kneber-botnet-netwitness-cybercrime**

25. "A new report by net security firm M86 Security points the finger of blame for the torrent of malware, phishing and other scams (collectively defined as malicious spam) and junk mail more generally towards botnet networks of compromised machines. It reckons five botnets were responsible for 78 per cent of spam in the second half of 2009"
http://docs.google.com/viewer?url=http%3A%2F%2Fwww.m86security.com%2Fnewsimages%2Ftrace%2FM86_Labs_Report_Jan2010.pdf&pli=1

26. "Let's start with the good news: Most computing devices and software became more secure in 2009. Increasingly, more vendors are starting to take computer security and patching seriously. Companies are making critical security patches available faster than in past years (across all platforms). More end-users are using auto-updating mechanisms to patch their OS and applications. The number of computers being applied with critical security patches is up. Responsible disclosure is up. Irresponsible, full disclosure is down. (See Figure 27 in the Microsoft Security Intelligence Report for the company's stats).The bad news on patching? Well, the fact that it's still so frequently and desperately needed across all OSs, all browsers, across nearly every very popular program. No one is expecting perfect code with zero vulnerabilities found over time, but it would be nice for patching to become a less regular event. The average end-user still has 12 unpatched programs... The average end-user patches his or her OS and doesn't patch his or her browser add-ins, which are

the ones most likely to allow malware onto a system". **http://www.mis-asia.com/opinion__and__blogs/bloggers/2009-marked-another-bad-year-for-it-security**

27."Information Commissioner found Verity Trustees Ltd to be in breach of the Data Protection Act after the Trustees reported the theft of a laptop containing the names, addresses, dates of birth, salaries and national insurance numbers of around 110,000 people. The laptop also contained the bank details of around 18,000 people, and was stolen from a locked room at the suppliers of the Trustees' pensions administration system".
http://www.ico.gov.uk/upload/documents/pressreleases/2009/verity_trustees_final_261109.pdf

28."The Information Commissioner's Office has found the **Association of Teachers and Lecturers (ATL)** in breach of the Data Protection Act after a laptop and memory stick were reported lost or stolen, containing the personal details of over 6,000 union members. ATL General Secretary, Mary Bousted, has now signed an Undertaking to ensure that all portable and mobile devices used to store and transmit personal details are encrypted" **http://www.ico.gov.uk/what_we_cover/data_protection/enforcement.aspx**

Appendix 4 Legal References

Indicative list of legal references. Following the links below will lead to more comprehensive references some of which are being updated regularly in light of current developments.

1. Irish Data Protection Acts. (Material extracted from website of Data Protection Commissioner) The main Irish law dealing with data protection is the **Data Protection Act 1988**. The 1988 Act was amended by the **Data Protection (Amendment) Act 2003**. An **informal consolidated version** of the two Acts is available.

The 2003 Amendment Act brought Irish law into line with the **EU Data Protection Directive 95/46/EC.**

All Sections of the Acts are in force, except Section 4 (13) (enforced subject access).

2. .Regulations under the Irish Data Protection Acts

Fees

S.I. 658 of 2007 - The fee you must pay for Registration and for Prior Checking
S.I. 347 of 1988 - The fee that an organisation may charge you for an Access Request(€6.35) and the fee for a certified copy of a Register entry (€2.54)

Registration

S.I. 657 of 2007 - Who must register
S.I. 351 of 1988 - Registration Forms
S.I. 350 of 1988 - Period of Registration (1 year)

Restrictions on Right of Access

S.I. 82 of 1989 - Health data
S.I. 83 of 1989 - Social Work data
S.I. 95 of 1993 - Functions of the Financial Regulator and of the Consumer Agency. Various functions performed by auditors etc under the Companies Acts
S.I. 81 of 1989 - Information on adopted children and information the Public Service Ombudsman gets during an investigation

S.I. 687 of 2007 - Processing of genetic data in connection with employment

3. Current Irish Electronic Privacy Regulations

The **ePrivacy Regulations 2003 (S.I. 535)** deal with data protection for phone, e-mail, SMS and Internet use. They give effect to the EU **e Privacy Directive 2002/58/EC.** These regulations have been amended by **SI 526 of 2008.**
SI 192 of 2002 – which has been replaced by SI 535 is available for reference.

4. Private Members Bill

http://www.oir.ie/viewdoc.asp?DocID=10087&&CatID=59&StartDate=01%20January%202008&OrderAscending=0

5. **Data Breach Notification Laws in Europe** Privacy Laws & Business: survey on attitudes of 21 European National Data Protection Authorities
www.privacylaws.com

6. Revised ePrivacy Directive
DIRECTIVE 2009/136/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:FULL:EN:PDF

7. Lisbon Treaty
" In accordance with Article 16 of the Treaty on the Functioning of the European Union and by way of derogation from paragraph 2 thereof, the Council shall adopt a decision laying down the rules relating to the protection of individuals with regard to the processing of personal data by the Member States when carrying out activities which fall within the scope of this Chapter, and the rules relating to the free movement of such data. Compliance with these rules shall be subject to the control of independent authorities".
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2008:115:0013:0045:EN:PDF

8. Article 8 of Charter of Fundamental Rights
"Protection of personal data

> Everyone has the right to the protection of personal data concerning him or her.
>
> Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
>
> Compliance with these rules shall be subject to control by an independent authority."

http://www1.umn.edu/humanrts/instree/europeanunion2.html

9. Stockholm Programme
Towards a Citizens' Europe in the area of Freedom, Security and Justice
The European Council reaffirms the priority it attaches to the development of an area of freedom, security and justice (JLS), responding to a central concern of the peoples of the States brought together in the Union.
http://register.consilium.europa.eu/pdf/en/09/st17/st17024.en09.pdf

10. Speech by Commissioner Reding
"It is my firm belief that we cannot expect citizens to trust Europe if we are not serious in defending the right to privacy . We need to ensure that personal data are protected against any unauthorised use and that citizens have the right to decide on the way their data are processed. Privacy and the protection of personal data have always been high on my list of priorities as the Commissioner for the Information Society."
http://register.consilium.europa.eu/pdf/en/09/st17/st17024.en09.pdf

11. Presentation by M. Renaudiere Data Protection Officer, EU Commission on current (February 2010) position of review of Data Protection Directive
"Challenges ahead for the Commission:

- need to clarify some key rules and principles: consent, transparency
- need to introduce new principles: privacy by design, accountability
- need to ensure protection regardless of the location of the controller
- need to strengthen enforcement
- need to limit bureaucratic burden"

http://www.lsec.be/upload_directories/documents/100209_DataProtection/3_Renaudiere_Philippe_EC_PerspectivesonDataProtection_1002009.pdf

12. 31st International Conference of Data Protection and Privacy (November 2009) an appraisal of some of the issues that are currently being discussed not only by the guarantors of privacy and data protection but by society at large, given the relevance for citizens of the decisions that are taken in this field. ..." The challenge we face as the organisers of the 31st International Conference is that of achieving the approval of a joint proposal on "International Standards for the Protection of Privacy and Personal Data", allowing the development of a universal, binding legal document, which must be backed by the most extensive institutional and social consensus via the participation of the authorities and institutions guaranteeing data protection and privacy and representatives of both public and private entities and organisations" **http://www.privacyconference2009.org/about_conference/index-iden-idweb.html**

13. EU Commission DG on Justice Law Security
http://ec.europa.eu/justice_home/fsj/privacy/index_en.htm

14. EU Commission Data Protection Officer
http://ec.europa.eu/dataprotectionofficer/index.cfm

15. **"The Future of Privacy: Joint contribution to the Consultation of the European Commission"** [by EU Data Protection Authorities] on the legal framework for the fundamental right to protection of personal data
http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2009_en.htm

16. **Article Reviewing potential impact of Lisbon treaty** "While much attention has been given to the Lisbon Treaty's reform of the EU's institutional arrangements, it also alters the legal grounds for legislation in the data protection area in ways that could impact privacy regulation. Below, we describe the key changes and consider the potential effect on Europe's data protection framework."
http://www.cov.com/files/Publication/44dd09f7-3015-4b37-b02e-7fe07d1403f4/Presentation/PublicationAttachment/8a89a612-f202-410b-b0c8-8c9b34980318/The%20Lisbon%20Treaty%20and%20Data%20Protection%20What%E2%80%99s%20Next%20for%20Europe%E2%80%99s%20Privacy%20Rules.pdf

17. Review of Data Protection Directive By UK Information Commissioner
http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/review_of_eu_dp_directive.pdf

18. Transfers of Personal data from the EU/EEA to third countries.
http://ec.europa.eu/justice_home/fsj/privacy/docs/international_transfers_faq/international_transfers_faq.pdf

19. House of Lords Report: **www.official-documents.gov.uk/document/cm72/7234/7234.pdf**

20. Australian reference "Office generally supports consideration of the addition of provisions to the Privacy Act to require agencies and organisations to advise affected individuals of a breach to their personal information in certain circumstances. Notification in a timely manner would enable individuals to take any necessary steps to protect their personal information. Such a change to the Privacy Act to require the reporting of information security breaches would provide a strong market incentive to organisations to adequately secure databases and information repositories to avoid the potential brand damage arising from negative publicity….. that 'mandatory reporting' legislation remains a new and evolving concept that requires further research. "

http://www.privacy.gov.au/publications/submissions/alrc/c11.html#L24947

21. New Zealand references "Notification can be an important mitigation strategy that has the potential to benefit both the agency and the individuals affected by the breach. If a privacy breach creates a risk of harm to the individual, those affected should be notified. Prompt notification to individuals in these cases can help them mitigate the damage by taking steps to protect themselves."
http://www.caslon.com.au/privacyguide5.htm

http://privacy.org.nz/assets/Files/Privacy-Breach-Guidelines/Privacy-breach-guidance.DOC

22. Canadian reference *Approaches to Security Breach Notification: A White Paper*, 9 January 2007 available at
http://www.cippic.ca/en/bulletin/BreachNotification_9jan07-print.pdf

23. USA reference Substantial recent Congressional report on Breach notification laws **http://opencrs.com/document/RL34120**

Appendix 5 Technical references

A set of indicative technical references. This is not intended to be comprehensive but illustrative of points made in the body of the report. References to organisations or products come from publicly sourced material.

1. "As computation continues to move into the cloud, the computing platform of interest no longer resembles a pizza box or a refrigerator, but a warehouse full of computers. These new large data centers are quite different from traditional hosting facilities of earlier times and cannot be viewed simply as a collection of co-located servers. Large portions of the hardware and software resources in these facilities must work in concert to efficiently deliver good levels of Internet service performance, something that can only be achieved by a holistic approach to their design and deployment. In other words, we must treat the datacenter itself as one massive computer." http://www.morganclaypool.com/doi/abs/10.2200/S00193ED1V01Y200905CAC006

2. "The IT environment has changed significantly in a few short years, as several factors have dictated the need for a more robust approach to corporate security policies, including:

1. A trend towards mobility of information,
2. Theft of IT assets arising from a proliferation of mobile devices,
3. Increasing data privacy and data security concerns, and
4. Regulatory compliance mandated by recent legislation.

These factors have made it necessary for network administrators to design and implement comprehensive security policies to keep pace with the changing IT landscape. Effective solutions for these multifaceted problems require a layered approach comprised of products, policies and procedures that can work in concert to provide organizations with the broadest security blanket available.

There is a strong relationship between the issues of compliance, data protection and theft recovery. Organizations must take this into account when defining security policies. It is no longer enough to attempt to address compliance issues without addressing data protection. Protection of data on mobile and remote computers requires an understanding of the issues surrounding computer theft" http://www.webbuyersguide.com/resource/white-paper/11429/Laptop-Security-Compliance-Protection-and-Recovery

3. "Is your system infected with a backdoor Trojan, or remote access Trojan? Maybe you received a warning from your antivirus, antispyware application, or someone helping you? What is a backdoor Trojan, and why should you be concerned?" http://www.geekstogo.com/2007/10/03/what-is-a-backdoor-trojan/

4. Report on US Federal Government skill shortage

http://www.theregister.co.uk/2009/07/22/federal_cybersecurity_shortage/

5. "The Symantec Internet Security Threat Report offers analysis and discussion of threat activity over a one-year period. It covers Internet threat activities, vulnerabilities, malicious code, phishing, spam and security risks as well as future trends. The fourteenth version of the report, released April 14, 2009, is now available". **http://www.symantec.com/business/theme.jsp?themeid=threatreport**

6. "A recent wave of cyber attacks that crippled thousands of computers and websites in the United States and South Korea could have originated from inside Britain, experts have warned. According to security researchers in Vietnam, the source of last week's string of attacks by the Mydoom virus - which overwhelmed systems belonging to the US Treasury and the office of the South Korean president Lee Myung-Bak - can be traced to the UK.....infected computers had tried to contact one of eight so-called command and control servers every three minutes....ordering them to direct traffic straight at victim websites, in attempt to overload them and force them to crash."**http://www.guardian.co.uk/technology/2009/jul/15/hacking-usa**

7. Analysis of a Botnet Takeover …..Once infected .. the victim host will join a botnet, which is a network of compromised machines that are under the control of a malicious entity, typically referred to as the botmaster. Botnets are the primary means for cyber criminals to carry out their nefarious tasks, such as sending spam mails , launching denial-of-service attacks, or stealing personal data such as mail accounts or bank credentials This reflects the shift from an environment in which malware was developed for fun to the current situation, where malware is spread for financial profit. **http://www.cs.ucsb.edu/~seclab/projects/torpig/torpig.pdf**

8. "The Petabyte Age is different because more is different. Kilobytes were stored on floppy disks. Megabytes were stored on hard disks. Terabytes were stored in disk arrays. Petabytes are stored in the cloud. As we moved along that progression, we went from the folder analogy to the file cabinet analogy to the library analogy to — well, at petabytes we ran out of organizational analogies." **http://www.wired.com/science/discoveries/magazine/16-07/pb_theory**

9. "In some ways, virtual server sprawl is much worse than the physical server sprawl from the turn of the last millennium. At least with real servers, there is some physical limit - the size of the data center and the power delivered to it - that puts a limit on the number of machines system administrators create."
http://www.theregister.co.uk/2008/11/10/sys_man_virt_cash/

10. "Adobe Insecure / Unpatched Version From Official Site"
http://secunia.com/blog/58/

11. "As attitudes to work and information continue to evolve away from those of the past, organizations are becoming more aware of the acute need to control the information that flows into, through and out of their networks. This paper demonstrates the need for a high-profile acceptable use policy to prevent data leakage, gives practical guidance on how to use current investments in IT security technologies at the gateway and endpoint to support this policy, and describes where new investment should realistically be made" **http://whitepapers.windowsecurity.com/whitepaper3127/**

12. Illustrative extract from sales material from one security solution vendor:

> " Attacks are typically targeting internal user systems within the corporate network, using invisible "Web-borne" techniques to take control. With the necessary tools readily available on the Internet, gaining remote access to an internal workstation only requires determination from the cyber criminal. It only takes a few hours for the criminal to stealthily gain access and take control of the critical internal business systems and data of a company and use them for profit".

13. Organized crime cells are especially focused on infiltrating businesses and personal computers, using the services of highly-skilled professional Crimeware writers. These crime pros need little time to access the personal information and data of the end-user. This of course significantly increases the security risk and thus places a huge burden on security experts. They use the Web as their main vector for malicious code propagation, since they understand that signature-based solutions were not designed to counter code obfuscation, Web 2.0 platforms and technologies, and other dynamic attack vectors in today's web scenario. " **http://www.wickhill.com/products/finjan/solutions/uk_index.php**

14. E-book- How to Secure Windows and Your Privacy. This open source ebook tells Windows users how to secure their computer and their privacy. **http://downloads.zdnet.com/abstract.aspx?docid=832667**

15. IT managers are "grossly underestimating" the explosion of unstructured data in the enterprise, according to Hewlett Packard. HP published new research carried out by Coleman Parkes Research, which surveyed more than 1,020 CIOs and department heads of large enterprise organisations across the UK and Europe. It found that on average, European companies believe than only 25 percent of their data is currently unstructured (i.e. emails, Word documents, third-party files). UK companies estimated that 29.4 percent of their data is in an unstructured format. This, says HP, is in stark contrast to research from industry analysts that indicate more than 70 percent of information is actually unstructured data. "Unstructured data is the 'dark matter' (i.e. the missing factor) of enterprise information **http://www.pcworld.com/businesscenter/article/153558/unstructured_data_grows_unchecked_study_says.html**

16. Sales material from vendor of cloud data holding: "Access all your backed-up data anytime from any Internet connection anywhere… Wherever there's an internet connection, you're a click away from any of your backed-up data. Just think of the convenience. " And the risk? **http://www.datadepositbox.com/index.php/data-backup-features**

17. "A devoted corps of companies pursues your data wherever you go, and they care nothing about your privacy. To coin a phrase, let's call them the *datarazzi*." **http://www.pebbleandavalanche.com/weblog?-quiet=1;page=45**

18. Vendor white paper on strategies to prevent Data Loss**.**
http://i.zdnet.com/whitepapers/Varonis_WhitePaper_10_Imperatives_for_Preventing_Data_Loss.pdf

19. “Specialist insurance products can mitigate the financial cost of any loss. E&O insurance provides cover for data loss as a result of negligence and is available from various Lloyd's syndicates, ... Companies can also take out a ‘cyber liability’ policy to cover defence costs and class actions from customers following a deliberate attack and these are also available from Lloyd’s, ... also arranges cover for small businesses and large corporations relating to data loss as a result of hacking, a virus attack or the theft of physical media. “Awareness of the risks associated with holding customers’ data has grown tremendously as a result of incidents like those at Nationwide and TJX,” ..Policies brokered include coverage for costs relating to reconstituting lost data and also the costs relating to third party claims following a breach of security. Policies also provide cover for the cost of notifying people about the incident and the legal costs involved in regulatory proceedings resulting from an incident. Lloyd’s insurers .... all write data loss related cover. A medium sized corporation can typically arrange cover with a limit of £25 million, though a programme of between £50 million and £100 million is possible in certain circumstances, ...” **http://www.lloyds.com/News_Centre/Features_from_Lloyds/Industry_wakes_up_to_data_loss_risk_07122007.htm**

20.“The business will look to its liability insurance for protection. However, businesses that are expecting coverage under their Commercial General Liability policy may be in for a rude surprise". **http://www.lctjournal.washington.edu/Vol1/a006Bodden.html**

21. "Employees routinely engage in activities that put sensitive data at risk. They are downloading data onto unsecured mobile devices (61%), sharing passwords (47%), losing data-bearing devices (43%), and turning off their mobile devices’ security tools (21%). And, reflective of the blurring of the lines between personal and professional lives, they are using web-based personal email in the office (52%), downloading Internet software onto an employer’s devices (53%), and engaging in online social networking while in the workplace (31%)". **http://www.ponemon.org/blog/post/more-employees-ignoring-data-security-policies**

22. "Some computer repair shops are illegally accessing personal data on customers' hard drives - and even trying to hack their bank accounts, a Sky News investigation has found" **http://news.sky.com/skynews/Home/UK-News/Sky-News-Undercover-Laptop-Investigation-Repair-Shops-Caught-Hacking-Into-Personal-Files/Article/200907315343387?lpos=UK_News_News_Your_Way_Region_5&lid=NewsYourWay_ARTICLE_15343387_Sky_News_Undercover_Laptop_Inve**

23. “The EDPS raises privacy concerns over the intelligent transport systems… The Commission believes that the deployment of ITS in Europe will serve different Community objectives such as cleaner transport, transport efficiency, improving safety and security. ….However, according to the EDPS, the Commission’s proposal is “too broad and general to adequately address the privacy and data protection concerns **http://europeanjournal.typepad.com/my_weblog/2009/07/the-edps-raises-privacy-concerns-over-the-intelligent-transport-systems.html**

Appendix 6 Regulatory references

Indicative list of references and sources. Following the links in the references below will lead to more comprehensive links.

1. "Better Regulation Website. The aim of this website is to provide information on Better Regulation - an important part of the Government's drive for greater economic competitiveness and modernisation of the Public Service. **http://www.betterregulation.ie/eng/**

2. Revised Regulatory Impact Analysis (RIA) Guidelines have now been published. These revised Guidelines take into account the recommendations from the Report on the Review of the Operation of RIA which was published in July 2008.

Risk Based Enforcement

3. Extract from a summary of work of High Level Group on Business Regulation:

> "One of the five Action Areas in the Government's strategy for economic recovery, Building Ireland's Smart Economy, is Efficient and Effective Public Services and Smart Regulation. The strategy states that "A consolidated inspections programme will be developed to reduce the number of inspection visits to business"; also that "Enforcement should be based on risk so as to minimise the burden on citizens and businesses."
>
> The High Level Group on Business Regulation is seeking ways to reduce administrative costs on business. The European Commission has found that cooperation with audits & inspection by public authorities, including maintenance of appropriate records accounts for more than half of all administrative costs, as measured in their cross-Community measurement exercise. In the UK, the Hampton Review of 20051 argues that pursuing a strictly risk-based approach to inspection and enforcement has the potential both to reduce administrative burdens on business and result in efficiency improvements in the Government sector."
>
> Key Points about Risk Based Enforcement
> The principle is that enforcement should aim to increase regulatory compliance in the most efficient and effective manner possible, given the limited resources available. Also that this should be done in such a way as to eliminate unnecessary administrative burdens in the economy.
> In order to achieve this, enforcement should be based on an assessment of risk. "The fundamental principle of risk assessment is that scarce resources should not be used to inspect or require data from businesses that are low-risk, either because the work they do is inherently safe, or because their systems for managing the regulatory risk are good."
> Risk assessment should use all available good quality data. Resulting enforcement activity should follow directly from this assessment. This means that inspections should be targeted where risk is greatest. In cases of low risk, advice and support may be sufficient to ensure compliance. In cases of persistent non-compliance, however, sanctions currently in place may not be sufficient to deter this behaviour, and may need to be reviewed.

> The cost to businesses of providing information and undergoing inspections should be weighed against the benefits deriving from this activity. In particular, the administrative burden imposed by regulators should be proportional to the risk associated with non-compliance. In practice, this may mean requiring less risky businesses to provide less information, for example. Enforcement should always include a small element of random inspection. It should also be dynamic in the sense that it responds to the best information available to regulators. The enforcement activities of different bodies should not overlap in a potentially confusing or duplicative manner."

4. The Financial Services Authority has fined HSBC £3m for failing to properly look after its customers' information and private data. These failures to follow proper processes led to at least two losses of customer data. The FSA investigated the bank and found unencrypted customer details on open shelves and unlocked cabinets. Customer details were also sent via the post or couriers to third parties **http://www.theregister.co.uk/2009/07/22/fsa_hsbc_data_loss/**

5. "The Information Commissioner's Office (ICO) has found Amicus Legal Ltd in breach of the Data Protection Act after reporting a laptop computer containing personal information relating to 100,000 customers was stolen. The laptop, privately owned by a contracted consultant, was not encrypted. Amicus Legal has signed a formal Undertaking outlining that it will take reasonable measures to keep personal information secure in future. The Undertaking has been signed on behalf of Amicus Legal Ltd by the Chief Executive, Andy Tomkins." **http://www.ico.gov.uk/upload/documents/pressreleases/2009/amicus_legal_undertaking_press_release.pdf** :

6. The Federal Trade Commission today released a survey showing that 8.3 million American adults, or 3.7 percent of all American adults, were victims of identity theft in 2005. Of the victims, 3.2 million, or 1.4 percent of all adults, experienced misuse of their existing credit card accounts; 3.3 million, or 1.5 percent, experienced misuse of non-credit card accounts; and 1.8 million victims, or 0.8 percent, found that new accounts were opened or other frauds were committed using their personal identifying information. **http://www.ftc.gov/opa/2007/11/idtheft.shtm**

7. US Government Accountability Office: Information Security. Agencies Report Progress but Sensitive Data Remain at Risk . **http://www.gao.gov/new.items/d07935t.pdf**

8. KPMG Survey on prevalence in UK :
http://www.kpmg.ie/Succeeding/publications/DataLossBarometer.pdf

9. Laptop Data Breaches: Mitigating Risks through Encryption and Liability Insurance Machal- Fulks & Scott
http://www.scottandscottllp.com/main/uploadedFiles/resources/Articles/Article-Laptop_Data_Breaches.pdf

10 The President's Identity Theft Task Force. Combating Identity Theft A Strategic Plan 2007 **http://www.idtheft.gov/reports/StrategicPlan.pdf**

11. "The influential Article 29 Working Party, an independent European advisory body on data protection and privacy to the EC, has argued that social networks like

Facebook, Twitter and MySpace need more regulation to ensure that personal data of their respective users is not put at risk. Even though the majority of sites that the report mentions are based in the United States, the group states their large presence in Europe means that they should be subject to European Union privacy and data protection legislation" **http://www.scribd.com/doc/16736099/ARTICLE-29-DATA-PROTECTION-WORKING-PARTY-Opinion-52009-on-online-social-networking**

12. Global Privacy Alliance - Data Breach Notification key points to consider
http://ec.europa.eu/justice_home/news/consulting_public/0003/contributions/organisations_not_registered/the_global_privacy_alliance_en.pdf