INNOVATION™
VALUE
INSTITUTE

Executive Briefing, August 2014

Dr John Ghent

Digital Risk Management and Data Protection

Digital Risk Management and Data Protection

IVI is researching the precise issues that increased use of technology is creating for businesses. As legislation grows, it is attempting to force organizations to measure and minimize the inherent risk. Data protection (data privacy) is a key focus which includes information security but much more. In this executive briefing we consider the issues around the development of a new DP capability and provide guidance to organizations that are attempting to measure and improve their capability to be compliant and manage risk.

KEYWORDS: Data Protection, Data Privacy, General Data Protection Regulation

Introduction

We live in a world that has benefitted greatly from the advances of technology, in terms of processing data and driving business strategy. Never before have organizations had the flexibility and capability that technology provides. However, this comes at a price. As organizations adopt more automation of processing, they become more dependent on technology. Similarly, as companies adopt more virtualization, cloud computing, and mobile and social media technologies they are fast losing sight of where their data is at any one time. A clear gap is emerging between capability and risk management. Current approaches cannot accurately describe an organization's capability to manage its data appropriately.

General Data Protection Regulation

Data Protection is a critical issue for companies for several reasons, not least that it is the law of the land to manage personal data appropriately. Recently, the European Parliament voted in favour of the new General Data Protection Regulation[1]. As this is a Regulation, and not a Directive, this law will come into effect once it is passed by the Council of Ministers. All indicators so far suggest that this Regulation could be enforceable as early as 2016. The Regulation will strengthen citizens' rights and compel companies to place more emphasis on the security and treatment of personal data.

One of the new proposals of the upcoming EU General Data Protection Regulation (GDPR) is the mandatory appointment of a Data Protection Officer (DPO) for companies processing the personal data of more than 5,000 data subjects in any 12 month period. In addition, individuals who wish to have their data deleted have the right to ask companies to be *forgotten*. Interestingly, in the two weeks since the European Court of Justice backed up a *right to be forgotten* request, Google received another 40,000 requests[1]. Individuals will also have the right to ask companies to transfer their data to a separate service provider. Not dissimilar to Subject Access Requests (SARs), this challenges companies to know where data is at all times, in both paper and electronic form. Companies will also be obliged to compile Privacy Impact Assessments (PIA) for any new projects that involve processing of personal data and where there is perceived risk to the personal data. The goal is to have privacy by default, rather than privacy as an afterthought. In certain situations, particularly where the PIA suggests there is a significant risk, the company (data controller or processor acting on behalf of the data controller) will have to consult with the Data Protection Commissioner to receive an authorization form permitting the data processing.

Interestingly, enforcement of the new Regulation currently proposes fines of up 5% of worldwide turnover for non compliance, which leads us to another critical reason for proper data management practices.

The Cost of a Breach

According to the latest report from Ponemon[6], an institute dedicated to researching privacy, data protection and information security, *the cost of a breach* is very significant. The study, which consisted of 314 organizations across 11 countries, reported that the average cost per lost record globally was $145, up 9% from last year. The most costly breaches occurred in Germany ($201 per lost record) and the USA ($195 per lost record). The average size of a breach was approximately 23,000 records.

Brand value also dropped between 17% and 31% following a breach, while the average brand loss was between US184 million and USD 330 million. Furthermore, a loss of 100,000 employee records would result in a 12% decrease in brand value. It is also worth pointing out that 59% of all breaches were caused by system glitches (business process failure) or human error. Malicious or criminal attack constituted just 42% of all breaches.

Assessing Data Protection Capability

We are in the process of developing a capability solely for Data Protection. Protecting the privacy and security of personal data is a critical component of any enterprise and currently there are no approaches developed to help organizations assess their data protection maturity, capability or compliance.

High level literature review

The International Organization for Standardization (ISO) has a few standards which are relevant here; namely ISO29100 and ISO29190. ISO29100:2011 describes a set of terminology that we will adhere to in the generation of the DP capability. It also specifies a set of 11 privacy principles, these are:

1. Consent and choice.
2. Purpose legitimacy and specification.
3. Collection limitation.
4. Data minimization.
5. Use, retention, and disclosure limitation.
6. Accuracy and quality.
7. Openness, transparency, and notice.
8. Individual participation and access.
9. Accountability.
10. Information security.
11. Privacy compliance.

ISO29190 builds on this set of principles to define an assessment model for an organization. While this standard is still in development, it requires the assessor to first collate a list of goals and processes prior to the assessment and lacks the detail a DP capability would provide through its CBBs and POMS.

An interesting development from the American Institute of Certified Public Accountants and the Canadian Institute of Chartered Accountants is the creation of the Generally Accepted Privacy Principles (GAPP). This consists of 10 principles from which a Privacy Maturity Model is developed around 73 criteria. There are significant gaps in this model around several keys areas which the DP capability will cover, ranging from leadership and strategy to staff management. Both these areas are of significant importance in determining if there is an appropriate budget in place for data protection and/or if your employees are more likely to be *ambassadors or assassins.* In addition, there are no Practices, Outcomes, or Metrics to reference in this model.

Extensibility as a Goal

The DP capability will cover all the material in ISO29100, ISO29190, and GAPP, but will go much further. It will help a company not only assess maturity to a greater degree of granularity but it will articulate the practices the organization needs to perform next, in order to move up the maturity curve. In addition, a key objective in the development of the DP capability is the extensibility of the model. We aim to develop the DP capability so that that we can add, for example, compliance tools on top of it. This tool could be specific to jurisdiction or standard.

Turning Compliance into a Business Advantage

While there are significant obligations on companies under the existing and new regulations, and significant financial threats to organizations that mismanage personal data, companies that embrace good data management practices will gain significant benefits. According to a recent EU press release, the value of European citizens' personal data will grow to over €1 trillion annually by 2020[8], leading many commentators and investors to the belief that *data is the new oil.* Crucially, the same rules will apply across the EU, which makes scaling a little bit easier. Companies can now select one jurisdiction and one data supervisory authority within the EU with which to deal and not have to liaise with potentially 31 different jurisdictions (28 EU states, plus Norway, Iceland, and Lichtenstein). Perhaps most importantly, companies with a high capability in data protection management not only greatly reduce the risk of a breach that could cause significant reputational damage but also increase efficiency and profits through appropriate and insightful use of the data.

Conclusion

Data protection best practice increases the usefulness of the data that an organization holds; it provides for higher quality analysis and more informed, compliant marketing. It minimises the costs of keeping and storing data, and introduces efficiencies within the flow of information throughout any company. Getting the right information to the right people in real-time is a by-product of optimized data management practices. The DP Capability will allow a company not only assess their level of compliance against standards and jurisdictions but will provide a framework and approach for maximizing the use of the personal data that they hold.

References

1. EU Data Protection website. http://ec.europa.eu/justice/data-protection/index_en.htm
2. International Organization for Standardization, 2011, ISO/IEC 29100:2011 Privacy Framework.
3. International Organization for Standardization, 2014, ISO/IEC DIS 29190 Privacy Capability Assessment Model.
4. McLaughlin, S. A. (2013, December). Using the IT-CMF as an Enabler for Transformational Change.
5. AICPA/CICA, 2009, Generally Accepted Privacy Principles.
6. AICPA/CICA, 2011, Privacy Maturity model.
7. Ponemon Institute May 2014, 2014 Cost of Data Breach: Global Analysis.
8. EU Press release http://europa.eu/rapid/press-release_MEMO-14-186_en.htm, 12 March 2014

About the Author

John Ghent is a managing partner of Sytorus, a leading data protection firm, and an IVI IT-CMF associate specialising in Data Protection. Prior to Sytorus, he was head of consulting for an IT firm with responsibility for growth, relationship management and technical oversight. John was responsible for the design and development of several national systems in Ireland and the UK. He holds a bachelor's degree with honours and a PhD in computer science from National University of Ireland, Maynooth. John attended Harvard Business School, completing an Executive Education Programme. He can be contacted at: *john.ghent@sytorus.com* or *john.ghent@nuim.ie*

This executive briefing was edited by Tom Keogan, TeKcomm Technical Writing.

About IVI

The Innovation Value Institute (IVI) is a multi disciplinary research and education establishment co-founded by the National University of Ireland Maynooth and Intel Corporation. IVI develops frameworks to assist IT and business executives to manage IT for Business Value and to deliver IT-enabled business innovation. IVI is supported by a global consortium of like minded peers drawn from a community of public and private sector organizations, academia, analysts, professional associations, independent software vendors, and professional services organizations.

Contact Us

For more information on IT-CMF and current IT hot topics, or on becoming a member of the IVI Consortium, please visit www.ivi.ie or contact us at:

ivi@nuim.ie or +353 (0)1 708 6931