Association for Information Systems
AIS Electronic Library (AISeL)

MCIS 2016 Proceedings

Mediterranean Conference on Information Systems (MCIS)

2016

Data Breach Notification: Issues and Challenges for Security Management

Maria Karyda
Dept. of Information and Communication Systems Engineering, University of the Aegean, mka@aegean.gr

Lilian Mitrou
University of the Aegean, L.MITROU@AEGEAN.GR

DATA BREACH NOTIFICATION: ISSUES AND CHALLENGES FOR SECURITY MANAGEMENT

Completed Research

Karyda, Maria, University of the Aegean, GR, mka@aegean.gr

Mitrou, Lilian, University of the Aegean, GR, L.Mitrou@aegean.gr

Abstract

Several high-profile personal data breaches have triggered a discussion among privacy advocates, security practitioners, corporate managers and politicians on what role regulation should play in how companies and organisations protect data. The self-regulation paradigm fails to reinforce individuals' right to information and foster proactive risk management as incident-related information is communicated informally and on a voluntary basis. Lately (April 2016) the European Parliament adopted a reformed General Data Protection Regulation (GDPR) which regulates data breach notification. This paper analyzes the current status in information security incident management, describes the data breach notification mandate introduced by the GDPR and discusses its impact on the accountability and transparency of organisations, the amplification of the security function in organisations and the security market and the reinforcement of situational awareness. This paper also identifies enablers and barriers to compliance and highlights the key challenges that governments and organisations need to address for effective incident management, in the context of the new regulation paradigm.

Keywords: General Data Protection Regulation, data breach notification, security incident, self-regulation, transparency, accountability.

1 Introduction

In 2014, hackers managed to get hold of the names, emails, addresses and phone numbers of 76 million households and 7 million small businesses by compromising about 90 of JPMorgan's servers, before being caught. Home Depot Inc had to pay about $19 million to compensate its customers affected by a massive data breach caused by a custom-built malware that resulted in the exposure of an estimated 56 million debit and credit card between April and September 2014. Back in 2008 an employee of the British Home Office misplaced a usb stick containing personal data of 84.000 prisoners, while one year earlier drug maker Pfizer informed about 17,000 past and present employees that their names and Social Security numbers had been exposed to potential unauthorized access. Among recent incidents the string of data breaches that suffered Sony Corporation were arguably the most high profile as in April 2011 hackers accessed personal information of its Playstation Network and Qiocity clients'. In 2014 alone the InfoWatch Analytical center registered 1395 cases of data leaks, citing that 350 million personal data records had been compromised due to insiders' actions and 410 million by external attacks. However individuals lack meaningful and efficient remedies against companies for the exposure of their information resulting from a data breach (Rancourt, 2011).

These high-profile data breaches and other data privacy issues have triggered a renewed and forceful discussion among privacy advocates, security practitioners, corporate managers and politicians on what role regulation should play in how companies and organisations protect data. In this context, a significant development has been the introduction of binding disclosure obligations after a security breach. Following USA[1] and Australia (Burdon et al. 2012, Esayas 2014), European legislators adopted the mandatory reporting of security incidents in several legislative texts regulating the electronic communications sector[2], the protection of personal data as well as cybersecurity[3]. European policy makers have tried to identify and introduce measures that aim at boosting security through regulation, such as the penalization of attacks, and also through understanding, management and mitigation of risks. An area of quite significant regulatory attention has been the introduction of binding disclosure obligations after a security breach. A data breach is the unauthorized or unintentional exposure, disclosure, or loss of sensitive personal information. These incidents deprive people of their right to confidentiality, privacy and integrity of their personal information. Most data breaches are currently a result of external actors such as hackers. Other sources include malware, social attacks, misuse by employees, physical action, errors and cyber espionage.

Initially, data breach notification was considered as "consumer privacy phenomenon". Due to the increasing number and complexity of attacks against information systems, however, security and data breach notification are currently viewed as a means to address the multifaceted problems of inadequate

[1] The first data breach legislation in the United States, was enacted in 2003 (California Civil Code § 1729.98) and became the basis for further legislative developments throughout the US. All but four US state-based legislatures have now enacted DBNL, which however vary in many elements from state to state (Bisogni, 2013).

[2] The Framework Directive imposed on providers the obligation to notify the competent national regulatory authority of a breach of security or loss of integrity that has had a significant impact on the operation of networks or services (Art. 13(a)(3)) while The e- privacy Directive as modified by included a framework for the reporting of data breaches to regulatory authorities and the potential notification of personal data breaches to affected individuals. The notification of personal data breaches under the ePrivacy Directive is replaced by the Regulation 611/2013.

[3] The reporting of security incident is introduced as means for obtaining of timely information about the occurrence, type and time for response to an incident of particular nature and also for facilitating a culture of collaboration between the private and the public sector (Draft Directive).

information security measures in organisations, the rapid increase of attacks, including identity theft crimes, and personal data protection (Burdon et al., 2012).

Organisations, however, tend to decline or avoid notifying their customers or employees that their personal data have been compromised, as they face an array of costs. Besides any direct costs associated with remedying security vulnerabilities that led to the security incident, companies are often obliged to spend money contacting customers, offering and paying for the services of credit reporting agencies, assisting law enforcement, business disruption expenditures, and litigation expenses. Besides the fear of costs by lawsuits, it has been found that when customers are informed about security incidents they are likely to avoid transactions in the future and switch to other providers. This behaviour is affected particularly by the significance of damage perceived by individuals as well as by existing alternatives (Lee and Lee, 2010).

The new obligations posed by the European legislation set a new scene for security management. Scholar research has currently identified the need to investigate not only the effectiveness of data breach notification laws but also to study its economic, legal, crime and security response effects (Bisogni, 2013). This paper addresses this need, by analyzing the implications of mandatory personal data breach notification for security governance of the Information and Communication Technology (ICT) infrastructure and incident response management in organisations. We focus on data breach notification imposed by the European General Data Protection Regulation (GDPR hereafter) as, due to the nature of the regulatory instrument and its territorial scope, it will have far reaching impact on security governance and incident management. The aim of this paper is to identify and explore the impact of the data breach notification mandate on security management and explore its role for enhancing accountability and transparency in organisations and its impact for society and individuals. We employ a multidisciplinary approach, to analyze both the legal framework and the technical aspects, with regard to the incident management and response strategies, security measures, policies and strategies that organisations use.

Through a multifaceted analysis, this study shows that data breach notification can enhance transparency and accountability of organisations, drive them to invest more on security, thus enforcing the market for data security technology. It can also empower security managers, increase security awareness and promote proactive security. It also poses new challenges as adopting common criteria for characterizing security incidents and evaluating incident management, developing and maintaining incident repositories and collaborating and sharing incident related information on a formal basis.

In the following section we describe the current state of security incident management in organisations under the self-regulation paradigm. Section 3 reports the provisions of the recently (April 2016) introduced General Data Protection Regulation (EC GDPR 2016) with regard to breach notification. In section 4 we discuss the impact of the data breach notification mandate on organisations, security management, governments, society and individuals. Finally we present our conclusions, highlighting key effects and open issues.

2 Background: Security management and Incident Response

The 2015 Information Security Breaches Survey reported that 90% of large organisations and 74 of small business had suffered a security breach that year, with an average cost of 1.46 to 3.14m pounds and 75k to 311k pounds respectively. However, only 39% of large organisations and 27% of small businesses have an insurance that would cover them in case of a breach. Furthermore, two-thirds of large organisations reported suffering from non-malicious or accidental breaches – the same level as last year – and one-quarter of small organisations suffered a similar type of incident (PWC, 2015).

Information systems security management is a critical activity that organisations employ to mitigate security incidents. It is part of a larger organisational process, information security governance, which employs technical, procedural, and human components by developing guidelines and implementing controls to address risks identified by the organisations (Da Veiga and Eloff, 2007). There are a number of widely subscribed management frameworks available that guide organisations in formulating and operating their information security efforts, including the ISO 27k (ISO/IEC 27000), COBIT 5 (COBIT) and the NIST Cybersecurity Framework (NIST, 2016), which prescribe technical, formal, and information security countermeasures.

The main strategic goal of security management in organisations has traditionally been to preserve the reliability of their ICT infrastructure, by preserving basic security attributes such the availability, integrity and confidentiality of the information while also preserving additional principles such as authenticity, accountability, non-repudiation, reliability and privacy from unwanted incidents. Although several security measures can be applied in order to prevent information security incidents from taking place, it is not economically feasible to fully protect all systems (Anderson et al., 2012). Thus organisations need to be able to manage security incidents in their ICT systems.

Information security incident management includes the processes for detecting, reporting, assessing, responding to, dealing with, and learning from information security incidents. In the context of security management a security incident is ‘‘a change of state in a bounded information system from the desired state to an undesired state, where the state change is caused by the application of a stimulus external to the system” (Stephenson, 2004). Thus, a security incident incorporates both the incident itself and the discovery of it. Suspicious events that appear to be incidents need to evaluated against certain predefined criteria so that further action is taken to mitigate security incidents and return computing resources to their normal state of functioning. ISO 27035 (ISO/IEC 27035:2011) has documented the following categories of security incidents: a) Denial of service incidents that prevent partial or complete access of networks, systems, or applications to legitimate users by exhausting resources; b) malicious code, including viruses, worms, Trojans and other code-based malicious entities that are inserted into other programs to modify their original content and function; c) inappropriate usage by authorized users who violate the information security policy; d) unauthorized access by non legitimate users who gain access to or misuse a system, service or network, and e) information gathering, which include activities linked with finding potential targets like vulnerabilities in the system or network that could be exploited.

Typically, the identification and reporting of an information security breach triggers a distributed and ah hoc process where a multitude of independent actors participate. Public officials and authorities, service providers, information security companies, research and volunteer organisations etc. are involved, co-operating mostly on a mutual trust basis, often through informal bilateral arrangements. As no entity controls the entire process, each participant assumes responsibility of their own actions resulting in a mesh of information sharing. A systematic approach to incident management is provided by the National Institute of Standards and Technology (NIST) in the US, which has published the ‘Special Publication (SP) 800-61 Revision 2, Computer Security Incident Handling Guide’ to assist organisations in establishing computer security incident response capabilities and handling incidents efficiently and effectively. According to this Guide, incident response management includes the following actions: create and incident response policy and plan, develop procedures for incident handling and reporting, develop guidelines for communicating with external entities relevant to the incident, staff and train an incident response team and establish communication channels between the incident response team and internal (e.g. legal department) and external (e.g law enforcement) groups.

The principal source of incident discoveries is local event monitoring, during which anomalous events are automatically detected and reported. Local event logging, however, loses track of incidents as soon as the attack has shifted to other systems and completely misses incidents that happen outside its scope, for instance attacks that exploit vulnerabilities similar to those existing in the local systems. An

alternative to event logging is to search for signs of specific attack patterns which have been previously known. Many organisations employ automated tools to automatically detect and report security incidents so as to reduce the critical time frame between the attack discovery and incident remediation. In many cases, organisations that suffer a data breach are notified by external entities, including Internet Service Provides (ISPs) and Computer Emergence Response Teams (CERTs). It is also often that external stakeholders who identify security breaches lack the communication channels to inform victims (Koivunen, 2010).

The discovery of an incident is followed by information exchange among involved parties and corrective actions. When the incident is under control its details need to be examined so as to enhance incident handling and security management. The final critical stage of incidence response management is a post-incident review. Post-incident reviews can bring real benefits to an organisation, including calculating the real costs of an incident, which in turn improves risk assessment. They also confirm whether mitigation efforts were effective or need adjusting, helping to ensure that attention and resources are focused where they're needed to properly manage risk, and lower the probability and impact of future incidents (Caldwell, 2012). Thus, incident management is largely based on various mechanisms for sharing experience, including different "lessons-learned" processes, like in-progress reviews, after-action reviewing and reporting. Their goal is to prevent the recurrence of adverse events and actions and to better contend with situations and problems that are likely to arise again. Incident evaluation is based on a systematic analysis, identifying the strengths to be sustained and the weaknesses to be corrected and also employing a learning process so as the newly accumulated knowledge is embodied in the organisation

Even when following standard guidelines and documented best practices however, incident response, especially in large organisations entails different groups working and collaborating in an ad hoc manner. One director of network forensics, describes: "*Traditional roles would include the firewall team looking at their logs, the intrusion detection team monitoring their information, the server team that would be responsible for looking for a potentially compromised server and pulling data off that, such as activity logs and then, obviously, the forensics team would be responsible for getting onto devices and doing a forensics analysis and finding out what has occurred on the device itself*." (Caldwell, 2012).

As a rule, companies under the self-regulation paradigm avoid going public with security incidents for fear of negative publicity, loosing their customers' trust, liability costs and adverse uses. This situation is changing, however, in the EU, due to the recent reform in the data protection regulation (EC GDPR, 2016)

3 New legal landscape: Breach notification in the General Data Protection Regulation

In the GDPR European legislators have extended the notification requirement beyond the electronic communications sector, while taking into consideration that "a personal data breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons …." (Recital 85). The GDPR defines a '"personal data breach" 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".

Adopting the so-called "risk based approach" [4] the GDPR limits the breaches to be notified only to these which are likely to result in a high risk for the rights and freedoms of individuals, such as discrimination, identity theft or fraud, financial loss, unauthorized reversal of pseudonymisation, damage to the reputation, loss of confidentiality of data protected by professional secrecy or any other significant economic or social disadvantage.

The breach has to be notified to the supervisory authority without undue delay and, where feasible, not later than 72 hours after having become aware of it and in case of delay the reasons therefore. Without undue delay the personal data breach is to be communicated also to data subject(s) while it is required to ascertain whether all appropriate technological protection and organisational measures have been implemented to establish immediately whether a personal data breach has taken place and to inform promptly the supervisory authority and the data subject (Rec.87). The communication should contain the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned, the likely consequences as well as the measures taken (or proposed to be taken) in order to address the breach. With regard to data subject the communication should include recommendations for the natural person concerned to mitigate potential adverse effect (Rec. 86).[5]

The communication to the data subjects concerned is not required if the controller has implemented appropriate technological protection measures, and that those measures were applied to the data affected by the personal data breach. Such technological protection measures should include those that render the data unintelligible to any person who is not authorized to access it, in particular though encryption. The other exemptions from notification to data subjects limit significantly the scope of notification obligation: the data controller is not obliged to communicate the breach also if:

a) he has taken subsequent measures that ensure that the high risk for the rights and freedoms of data subjects is no longer likely to materialize,

b) the notification would involve disproportionate effort, in particular owing to the number of cases involved. In such case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner; or

c) the notification would adversely affect a substantial public interest. This is the case for example if an early disclosure could unnecessarily hamper the investigation of the circumstances of a personal data breach (Recital 88)

4 Analyzing the implications of the data breach notification mandate

The data breach notification mandate can support affected entities and individuals to mitigate the harm caused by the breach. The effective implementation of this newly adopted legislative require-

[4] A common view emerged during the discussions on the GDPR in the Council was that the risk inherent in certain data processing operations should be a main criterion for calibrating the data protection obligations. Where the data protection risk is higher, more detailed obligations would be necessary and where it is comparably lower, the level of prescriptiveness can and should be reduced proposals to implement a strengthened risk-based approach in the text of the Regulation At the Council of March 2013, there was a large agreement on the need to reduce burdens on enterprises, in particular regarding small and medium-sized enterprises and the drafting of the Regulation was based on the risk-based approach, inter alia, by further developing criteria for enabling the controller and processor to distinguish risk levels .

[5] With regard to the scope and the content of notification the e- Privacy Directive provides also that notifications to subscribers or individuals should at least include the nature of the breach, relevant contact points to gain further information and the recommendation of further measures to mitigate adverse effects of the breach.

ment in Europe, however, relates also to the identification of impacts of notification model features on the social environment, businesses and citizens.

4.1 Issues and challenges for organisations

Security breach notification legislation is related to the approach of "governance through transparency" or "regulation through disclosure" and is associated with the community's "right to know" regulation laws, which was developed in order to improve the efficacy of environmental laws (Esayas, 2014). As noted by de Hert and Papakonstantinou (2016), the principle of transparency is of paramount importance in the data protection field as processing operations do not take place in public, nor their results are felt immediately by the individuals concerned. This is the case for personal data breaches too.

Transparency in its turn should raise the level of accountability. Accountability involves committing to legal and ethical obligations, policies, procedures and mechanisms as well as explaining and demonstrating implementation to internal and external stakeholders and remedying any failure to act properly. According to the GDPR (art 5 (2)), data controllers shall be responsible for, and be able to demonstrate compliance with the principles of data protection and the law (EC GDPR 2016). Enhancing an organisation's accountability improves its ability to respond timely, effectively and rigorously to security risks and incidents. Some authors underline that social reporting practices may create the "appearance of accountability" without any substantial impact on organisation's behavior and their accountability to the individuals concerned. They warn of the risk that reporting may divert attention away from potentially more effective means of accountability (Hess, 2005)

With regard to the economic effect, it is generally the case that breach notifications have a negative impact on customer loyalty. According to a recent study (Ponemon Inst., 2012), 15 percent of respondents will terminate their relationship after a breach notification and 39 percent will consider ending the relationship. 35 percent reported that their relationship and loyalty is dependent upon the organisation not having another data breach. Besides customer loss, another direct economic effect is linked to the possible decrease of firm market value subsequent to a security breach. Garg et al (2003) report the case of firms victimized by a security breach involving theft of credit card information that suffered a stock market loss of 9.3 percent on the first day the breach was announced, increasing to 14.9 percent over three days.

Without any doubt, mandatory notification is costly for organisations as they have to organize customer services operations and redress and they have to take into account also legal fees, potential administrative sanctions (fines) for non compliance with their security obligations[6] as well as potential loss of market value due to reputation harm. On the other hand as data breach notification may cause the individuals concerned to take action for mitigating the risk and reducing harm, this can result into lowering an organisation's own expected costs (Bisogni, 2012).

However when disclosure costs are high for companies and organisations they will be induced to invest more in security. The only factor that has a significant and positive impact on cost expectations is risk of harm to business from breaches in security or other data security concerns (London Economics, 2013). Personal data breaches seem to be more damaging to companies than other security breaches. Campbell et al. (2003) found that security breaches in which personal data was accessed had a significant impact on a company's stock market valuation. Furthermore, among personal data breaches, those

[6] The implementation of appropriate organisational and technical measures to ensure confidentiality and security of processing of personal data is a requirement laid down both in the Data Protection Directive in force (Articles 16 and 17) and the General Data Protection Regulation (Art. 32).

that involve financial data tend to result in larger share price reactions as might be expected, given the value of the information and including the effect of liabilities arising from legal claims in the future.

4.2 Issues and challenges for security management

At the organisation level the effectiveness of security management and incident response are related to organisational characteristics such as the quality and number of human resources (including information security staff, security training and awareness on various security aspects), to specific company internal elements, including security technologies and procedures in place, information sharing, managerial, technical, and operational controls, and finally to presence of specific insurance. Other elements that contribute to a company's readiness to invest in the prevention of security breaches include the size and type of business and the type of information involved (Bisogni, 2012). In this context breach notification laws can contribute to enhance awareness of the importance of information security across all organisational levels as the legal obligation may empower information security personnel to implement new access controls, auditing measures, and encryption. The legal mandate can also empower security managers claim resources for effective security and justify their cost. Moreover, due to the increased scrutiny of their activity and their possible liability, security management in organisations is expected to respond more effectively and rigorously to threats and breaches. As ICT security controls of are in some cases foreseen and imposed by the law, the breach notification can enhance the impact of mandatory security obligations and ensure compliance with them.

Furthermore, apart from any organisation's own efforts to comply with breach notification laws, reports of breaches from other organisations help information officers maintain a proactive approach to risk management. Not all companies are however expected to react to the breach notification mandate in the same way. The criteria that will be perceived as relevant by an organisation when taking a decision about its level of security and related investments are also influenced by its business model and by the sector it belongs to. For instance, commercial organisations will primarily respond to incentives that have direct and indirect implications for their profit, while financial and insurance services companies are more likely to adhere to the new mandate as they already operate in strongly regulated sectors (Bisogni, 2012).

Breach notification regimes appear to have a preempting function: The breach notification requirement is expected to increase the situational awareness inside organisations that allows a better evaluation of security risks. Incident information disclosure is an essential part of crisis communications, which can "*reduce and contain harm, provide specific information to stakeholders, initiate and enhance recovery, manage image and perceptions of blame and responsibility*" (Kulikowa et al., 2012). The Data breach notification framework can be conceived as a part of regulatory strategy which encompasses also data protection impact assessments and privacy by design requirements; by complying organisations also manage to address security issues in advance, during the security risk analysis and processing design phase, thus avoiding a possible last minute rush and confusion in determining which risks to report once a security breach occurs.Another effect is that, relevant provisions concerning notification of data breaches provide controllers with an incentive to comply both with technical and legal standards and requirements (Eckhard and Schmitz, 2010).

As mentioned previously, exemptions of the data breach notification mandate allows data controllers to assess the severity of risk and the level of damage and, moreover, to implement measures and avoid notifying the individuals concerned (de Hert and Papakonstantinou, 2016). Organisations will be therefore compelled to employ further security measures to limit and or to reduce the damage. As abovementioned, the law motivates data controllers to take subsequent measures that ensure that the high risk for the rights and freedoms of data subjects is no longer likely to materialize as in this case they have not to confront themselves with the impact of a notification that could result into the "shaming" of the controller who failed to undertake appropriate security measures.

Another challenge for security management is the determination of the criteria to characterize data breach events. Currently, these criteria vary from country to country and from organisation to organisation, depending also on the understanding and distinction of security events and incidents. This problem is also illustrated by terminological inconsistencies: the European Network and Information Draft Security Directive (NIS Draft Directive, 2013) refers to the notification of "incidents", whereas the GDPR calls them "breaches of security". Organisations compliant to ISO/IEC 27035:2001 for instance treat actions such as the automated pinging of their network addresses or scanning the available network ports of their systems as a security incident. This, however, could not be considered as a personal data breach case.

Following the GDPR, providers are required to maintain an inventory of data breaches that includes the material facts, the effects of the breach and remedial action taken that is provided to national regulators. This documentation shall enable the supervisory authority to verify compliance with the law. This requirement ensures the transparency and allows the assessment of this notification model while enabling national authorities to verify compliance with the law. It also, poses, however, new challenges with regard to additional costs for maintaining and securing the inventory, as wee as interoperability issues.

Article 4(3) of the GDPR contains a general exception to subscriber or individual notification if the provider can demonstrated to the satisfaction of the competent authority that it has implemented appropriate technological protection measures to render the data unintelligible to any person who is not authorised to access it and those measures were applied to the data concerned by the security breach. However, the scope and time frame in which "data is unintelligible" is subject to resources, technology etc and need further clarification for security management.

Finally, with regard to the scope and the content of notification, the e- Privacy Directive leaves national legislators a large degree of interpretation. The Directive specifies neither the form nor the substance of notification providing however that, notifications to subscribers or individuals should at least include the nature of the breach, relevant contact points to gain further information and the recommendation of further measures to mitigate adverse effects of the breach.

4.3 Issues and challenges for society and individuals

The notification of breaches to individuals, in case that they are affected thereby, reinforces their right to information, which is a fundamental principle of the EU legal framework.

Transparency is a crucial pillar of an efficient data protection that is already under the scope of the Data Protection Directive (Data Protection Directive 95/46/EC). Currently, under the self-regulation paradigm the achievement of transparency, for the limited number of organisations that do inform their clients in case of data breach voluntarily is hindered by the lack of verification, as there are practically no means to ensure the accuracy and completeness of information provided for external accountability (Bonner, 2012). Breach notification regimes may help individuals to mitigate the damages of a breach by compelling the notifying organisation to suggest some measures in order to mitigate the harm. Breach notification legislation is also expected to increase the level of security and foster trust among citizens in how their data is being dealt with, secured and protected by companies who handle their personal data. The approach of "governance through transparency" or "regulation through disclosure" can also affect the level of accountability. Accountability involves committing to legal and ethical obligations, policies, procedures and mechanisms as well as explaining and demonstrating implementation to internal and external stakeholders and remedying any failure to act properly

The imperative for effective security, so as to be exempted for breach notification, is also expected to drive forward the market for data security technology.

4.4 Issues and challenges for governments

The GDPR raises the need for a common incident management system across European states for a coordinated response and access to the resources necessary for successful risk mitigation. Despite the fact that currently CERTs in different European countries collaborate and the existence of the CERT-EU building and maintaining a common incident response and management system will facilitate effective risk mitigation but raises many political, legal as well as organisational and technical issues. Governments, however, need to foster learning and collaboration for incident response and investigation among all stakeholders involved, including public authorities, private organisations, individuals etc.

On the other hand, concerns are expressed with regard to the risk of excessive and / or counterproductive notification which could give rise to notification fatigue. A possible flood of notifications would result in ignoring the really important warnings. This argument seems to be supported by as survey, which found that consumers do not pay sufficient attention to the notices they receive with over 36% of respondents taking their breach notification letter as a junk mail whereas 13% of respondents taking their breach notification email as spam (Ponemon Inst., 2012)

5 Conclusions and further research

Security management and incident handling need to adapt to a changing technical and legal landscape where ICT threats are transient, unpredictable and difficult to measure, effective security controls need to be emergent and are dynamically connected to the threats (Baskerville, 2014) and the notification of personal data breaches becomes a legal mandate under the European General Data Protection Regulation.

Incident-response capabilities are vital for organisations to quickly respond to and recover from security-related incidents such as viruses or intentional breaches of computer networks. As there is not up-to-now a generally accepted method of evaluating ICT security incident management, it is hard to make concrete comparison with regard to the effect of the new European data protection regulation. This paper provides an analysis of the impact of data breach notification mandate with regard to organisational, security and economic aspects and identifies barriers and enablers to incident management and critical points for governments, organisations, society and individual. We have identified critical factors that are likely to influence the compliance with the new regulation and discuss how security incident management can be enhanced. Our analysis shows that breach notification can increase security awareness in organisations, allow better evaluation of security risks, increase transparency and enforce the right of individuals to be informed on their personal data. It can also empower security managers to justify expenses on protecting their systems and drive organisations integrate an incident response /management system in their ICT infrastructure. The big challenge for security now will become to shift the main goal of security governance and management from reliability to fostering accountability and transparency. The imperative for effective security, so as to be exempted for breach notification, is also expected to drive forward the market for data security technology.

Security management research and practice need to define criteria on characterizing data breaches and security incidents and also need to develop a framework for evaluating incident management. Sharing of incident related information is a key factor to achieve proactive security management and identifying the right channels and ways to communicate with data subjects is critical for limiting the negative impacts of breach notification. Maintaining an inventory of data breaches, as the GDPR regulates promote information sharing and proactive security but at the same time raises additional costs, security concerns and interoperability challenges.

There is also a need for provisioning a “public register” of breach events that could be kept by the supervisory authority. This register, which is provided in the related legal instruments, may burden the

competent authorities, but on the other side it could be a step towards transparency and accountability. Building a body of this knowledge can be of value for both states and organisations and improve cyber incident notification; however it is still an open issue.

References

Anderson R, Barton C, Bohme R, Clayton R, Eeten M, Levi M. Measuring the cost of cybercrime. In: Proceedings of the 11th Workshop on the Economics of Information Security (WEIS'12); 2012.

Baskerville R., Spagnoletti P and Kim J. (2014) Incident-centered information security: Managing a strategic balance between prevention and response, *Information & Management*, 51 (2014), 138-151

Bonner L., (2012), Cyber Risk: How the 2011 Sony Data Breach and the Need for Cyber Risk Insurance Policies Should Direct the Federal Response to Rising Data Breaches, Washington University Journal of Law & Policy, Vol. 40

Burdon, M, Lane, B and von Nessen, P, (2012), 'Data Breach Notification Law in the EU and Australia – Where to Now?' 28(3), *Computer Law and Security Review*, 296

Caldwell T. (2012), "Prepare to fail: creating an incident management plan", *Computer Fraud & Security*, Nov. 2012, pp10-16.

Campbell, K., Gordon, L., Loeb, M. and Zhou, L. (2003), 'The economic cost of publicly announced information security breaches: Empirical evidence from the stock market', *Journal of Computer Security*, 11, 3, 431–448

COBIT 5, available at http://www.isaca.org/cobit

Data Protection Directive 95/46/EC http://eur-lex.europa.eu/

Da Veiga A., and Eloff J. H. P., (2007), An Information Security Governance Framework, *Information Systems Management*, 24:4, 361-372

de Hert P. and Papakonsantinou V. (2016), The new General Data Protection Regulation: Still a sound system for the protection of individuals?, *Computer Law & Security Review*, Volume 32, Issue 2, April 2016, Pages 179–194

Eckhard J. and Schmitz P., (2010), "Informationspflicht bei Datenschutzpannen" 34, Datenschutz und Datensicherheit 390-397

Esayas S. (2014), Breach Notification Requirements Under the European Union Legal Framework: Convergence, Conflicts, and Complexity in Compliance, 31, J. Marshall J. Info. Tech. & Privacy L, p. 319 with further references

Garg A., Curtis J. and Halper H., (2003) "Quantifying the financial impact of IT security breaches," *Information Management & Computer Security*, 11/2: 74-83.

European Council EC (2016), General Data Protection Regulation, available at http://www.consilium.europa.eu/

Hess D. (2005), Social Reporting and New Governance Regulation: The Prospects of Achieving Corporate Accountability through Transparency, SSRN, available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=818544

ISO/IEC 27035:2011 Information technology — Security techniques — Information security incident management

ISO/IEC 2700, Information Security Standards, available at http://www.iso27001security.com/index.html

Koivunen E. (2010). "Why wasn't I notified?" Information security Incident Reporting Demystified, Proceedings of the 15th Nordic Conference in Secure IT Systems, 2nd Edition. London: McGraw-Hill.

Kulikowa O., Heil R., den Berg J. Pieters W. (2012), Cyber Crisis Management: A decision-support framework for disclosing security incident information, in Proc. of the 2012 International Conference on Cyber Security, IEEE

Lee M. and Lee J. (2010), The impact of information security failure on customer behaviors: A study on a large-scale hacking incident on the internet, *Information Systems Frontiers*, April 2012, Volume 14, Issue 2, pp 375-393

London Economics (2013) Implications of the European Commission's proposal for a general data protection regulation for business, Final report to the Information Commissioner's Office

NIS Draft Directive (2013), European Network and Information Draft Security Directive, http://eur-lex.europa.eu/

NIST (2016), NIST Cybersecurity Framework, available at http://www.nist.gov/

Ponemon Institute LLC, (2012), *Consumer Study on Data Breach Notification*, June 2012, available at http://www.experian.com/assets/databreach/ brochures/ponemon-notification-study-2012.pdf.

PWC (2015), Information Security Breaches Survey, available at http://www.pwc.co.uk/services/audit-assurance/insights/2015-information-security-breaches-survey.html (accessed May 2016)

Rancourt S. J. (2011), Hacking, Theft, and Corporate Negligence: Making the Case for Mandatory Encryption of Personal Information, 18, *TEX.WESLEYAN L. REV*. (2011), p. 186

Stephenson P., (2004) Managing digital incidents – a background, *Computer Fraud &Security* (12), 2004, pp. 17–19.