Digital Investigation 24 (2018) S93–S100

Contents lists available at ScienceDirect

Digital Investigation

journal homepage: www.elsevier.com/locate/diin

DFRWS 2018 Europe — Proceedings of the Fifth Annual DFRWS Europe

A comparative study on data protection legislations and government standards to implement Digital Forensic Readiness as mandatory requirement

Sungmi Park [a], Nikolay Akatyev [b], Yunsik Jang [a, *], Jisoo Hwang [c], Donghyun Kim [c], Woonseon Yu [c], Hyunwoo Shin [c], Changhee Han [c], Jonghyun Kim [d]

[a] Institute of Legal Informatics and Forensics Science, Hallym University, Chuncheon, South Korea
[b] Horangi Cyber Security, South Korea
[c] Best of the Best (BoB), Korea IT Research Institute, Seoul, South Korea
[d] DOUZONE Forensic Center, South Korea

Keywords:
Incident response
Digital forensic investigation
Digital foresic readiness
Data protection legislation
Minimum security standards

A B S T R A C T

Many data breaches happened due to poor implementation or complete absence of security controls in private companies as well as in government organizations. Many countries work on improvement of security requirements and implementing them in their legislation. However, most of the security frameworks are reactive and do not address relevant threats. The existing research suggests Digital Forensic Readiness as proactive measures, but there is only one example of its implementation as a policy. Our work surveys the current state of data protection legislation in the selected countries and their initiatives for the implementation of Digital Forensic Readiness. Then we discuss if Digital Forensic Readiness as a mandatory requirement can improve data protection state in both public and private sectors, evaluating possible challenges. We contribute suggestions for the adoption of Digital Forensic Readiness as a mandatory requirement for private companies and government organizations.

Introduction

Several researchers (Tan, 2001; Baek and Lim, 2012; Endicott-Popovsky et al., 2007) discuss a model for Digital Forensic Readiness (DFR). To the best of our knowledge, only the work of Mouhtaropoulos et al. (2011). guides the formulation of a Digital Forensic Readiness policy. The work includes a comprehensive analysis and suggests relevant policies, but it is outdated and only covers the most representative countries of the Commonwealth, the UK, Australia, and Canada, along with the US.

Our work builds on the foundation of (Mouhtaropoulos et al., 2011) and reflects dynamic developments of the policies in the technical world. Together with the US and the UK, we include EU with the example of Germany and South Korea in our analysis. It is not the purpose of this paper to recap the suggestions of DFR models and provide a new model. Instead, this paper is specifically designed to discuss the effectiveness of the current data protection legislation, the impact digital forensics has in the information security field and if it would be beneficial to implement Digital Forensic Readiness in a mandatory way. Each country is in a different state of promoting digital forensics and Digital Forensic Readiness as part of their information security guidelines, which is the focus of this paper. The final goal is to examine the benefits of integrating Digital Forensic Readiness as a component in the data protection legislation following the UK example and ultimately to suggest companies in the private sector to consider implementing Digital Forensic Readiness in their information security policies.

In this paper, Digital Forensic Readiness (DFR) will follow the definition suggested by Tan, Rowlingson, Grobler and others (Tan, 2001; Rowlingson, 2004; Grobler et al., 2010; CESG, 2015); Digital Forensic Readiness refers to the ability to maximize the usage of digital evidence, so the cost of an investigation can be minimized. Digital Forensic Readiness' basic objectives are to maximize an organization's ability to collect and use (admissible in court) digital evidence and to minimize the cost of forensics on incident response (Tan, 2001). It is considered as proactive digital forensics, a term understood as setting up systems so if an incident occurs, the evidence will be maximized (Bradford et al., 2004). Other researchers, such as Danielsson & Tjostheim, have moved the concept of

* Corresponding author.
E-mail address: jakejang@hallym.ac.kr (Y. Jang).

https://doi.org/10.1016/j.diin.2018.01.012

security to the cyberspace. According to them, Digital Forensic Readiness is comparable to the physical measures organizations take to deter, detect, or provide information about events, such as CCTVs or building entry logs (Danielsson and Tjostheim, 2004). The CESG defines Digital Forensic Readiness as an appropriate level of capability by an organization to be able to collect, preserve, protect and analyze legally sound digital evidence (CESG, 2015).

In this paper, we approach the problem comparing existing data protection legislation and analyzing their weaknesses. We discuss whether the mandatory adoption of Digital Forensic Readiness in the existing information security framework can overcome these problems.

The rest of the paper includes the comparative analysis of data protection legislation in the US, UK, EU and South Korea. It is followed by a review of initiatives in this countries for the implementation of Digital Forensic Readiness. Section Case study: implementation of Digital Forensic Readiness as mandatory requirement in the UK gives a case study of the mandatory requirement to the adoption of DFR by the government in the UK. Based on the reviews and the case study, section Discussion: future directions for implementation of Digital Forensic Readiness as mandatory requirement suggests the implementation of DFR as a mandatory requirement in other countries as well as discovers potential challenges. Section Conclusion concludes the paper and suggests directions for future work.

Comparative analysis of data protection legislation in the US, UK, EU and South Korea

In this section, we will discuss the legal security requirements in different countries to estimate the necessity of increased, legally mandated data breach preparation.

The United States

The US does not have a single unified comprehensive data protection law. Multiple federal laws partly mention activities such as ensuring privacy, securing data, or notifying users of data breaches. The relevant federal laws are mostly categorized by the type of the data each tries to protect. This includes HIPAA (Health Insurance Portability and Accountability Act) and HITECH (Health Information Technology for Economic and Clinical Health Act) for healthcare data, Gramm-Leach-Bliley Act for financial data, and Children's Online Privacy Protection Act for information obtained from children. SOX (Sarbanes-Oxley Act) also has a place in data security in the field of corporate governance.

At the federal level, most legislation addresses the responsibility of the data owners to reasonably secure themselves from data breach (Zurich, 2010). Section Review of initiatives in the US, EU, Germany and South Korea for the implementation of Digital Forensic Readiness of the Data Security Act of 2014 states "… implement, maintain, and enforce reasonable policies and procedures to protect the confidentiality and security of, sensitive account information and sensitive personal information …" (S 1927), referring to the security responsibility of businesses, financial institutions, entities or individuals that maintain or otherwise possess the information. However, it is questionable whether those standards are enough to prompt organizations to invest in sufficient information security. One of the telltale signs, that suggest a deficient security net, could be the low success rate of negligence lawsuits based on the mandatory safety lines.

Compensation out of negligence has four components that need to be proven: (1) legal duty of the defendant to protect the plaintiff's data, (2) proof that the defendant has failed its duty to reasonably secure the data, (3) proof that the defendant's breach caused (4) a "cognizable" injury to the plaintiff (Kosseff, 2017). The first component is relatively easier to prove than the rest, as it can be derived from the law, protocol, or contract with the consumers. The second component can be trickier. What is considered "reasonable" in the US has no uniform answer yet (Fisher, 2013). A possible solution is using international controls such as the ISO 27001 certification. However, as such standards are not mandatory, many businesses are still left vulnerable.

In the Sony data breach litigation, one of the few successful data breach lawsuits, the court found Sony's security standards severely lacking, showing that the files were not encrypted or password-protected, and determined that Sony had the legal responsibility and had failed to prevent the breach (Tsotsis, 2014). The Target data breach litigation resulted in a similar process this time the fault lied in the inadequate reaction of personnel.

While this lawsuit was successful in a legal sense, it does not ensure better security in the future. In fact, Target had paid less than 50 cents on average per victim based on 11 past data breach settlements, for cases involving more than 1 million victims (District of Minnesota, 2015). Compensation is a legal mechanism that ultimately aims to protect the plaintiff by reinstating their losses and serving as a penalty to the defendant. However, in the previous data breach litigations, the results do not seem to serve either purpose. The compensation in the Target case was so low victims decided to settle for non-monetary promises such as updating the company's security instead (Rossi, 2015). In the long term, low, weak standards of security and low fines will lead to low interest, resulting in subpar data protection. This reflects how far behind the importance of promoting information security is in the current legal system.

Since the Target breach and other data breach incidents, some voices in Congress are considering implementing a federal set of standards that would be applicable to businesses (Fisher, 2013). Currently, standards for security are either distributed throughout the state, community or organization, resulting in a sort of security patchwork. Without a comprehensive standard, however, it will not be possible to prevent incidents that have an equal effect throughout the country.

The United Kingdom

Government departments and agencies in the UK must adhere to the legal requirements in the Security Policy Framework (SPF) (Cabinet Office, 2010), as such measures are fundamental to ensure improved public services and efficient, effective and safe conduct of public business (Mouhtaropoulos et al., 2014).

Since 90s (Mouhtaropoulos et al., 2011) the government has been implementing different legislations related to information security, but a major incident in 2007 fostered the government to adopt Her Majesty's Government (HMG) Security Policy Framework in 2008 (Poynter, 2008). Also known as the HM Revenue and Customs (HMRC) incident, the government was responsible for the loss of the personal records of 25 million individuals, which included date of birth, addresses, bank accounts and national insurance numbers (Wintour, 2007). The breach of faith between state and citizen that made half of the British population vulnerable to the threat of fraud and theft resulted in a highly alerted government to invest in better, more efficient security rules.

The key factors that led to the breach were found to be the lack of information security awareness across the staff and lack of adhering to the HMRC security guidelines (Poynter, 2008). As the demand and necessity of minimum security requirements kept growing, the Cabinet Office then released a report called "Cross Government Actions: Mandatory Minimum Measures", enumerating 22 minimum mandatory requirements, including Digital Forensic Readiness, that would apply to all governmental