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 The work includes a comprehensive analysis and suggests relevant policies, but it is outdated and only covers the most representative countries of the Commonwealth, the UK, Australia, and Canada, along with the US.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

departments. In 2010, the Cabinet Office published the "HMG Security Policy Framework", covering mandatory security policies in details. Information Security and Assurance policies included policies such as informative security policies or annual technical risk assessment, having trained personnel as accounting officer, ability to regularly audit information assets and ICT systems, and other technical requirements (Cabinet Office, 2010).

SPF establishes mandatory implementation of information security management in government departments but recommends as best practices to the private sector.

EU

According to the General Data Protection Regulation (GDPR) Article 32, the affected organizations need to implement appropriate technical and organizational measures for data protection, while "taking into account the *state of the art*". In the case of non-compliance, Article 83 of GDPR imbues fines up to an amount that is greater than 10,000,000 EUR or 2% of global annual turnover (GDPR Report, 2017). It can be even higher if the non-compliance is related to key provisions; the fine goes up to 20,000,000 EUR or 4% of global annual revenue, depending on which one is greater (GDPR Report, 2017).

Due to its heavy fines and stricter regulations, compliance with GDPR is of the utmost priority for affected organizations. Therefore, full comprehension of the term "State-of-the-Art" in the context of the GDPR is important to be able to prepare security measurements.

However, even with this interpretation, many organizations are still concerned about the ambiguity of the legal security standard. Especially since GDPR Art. 82 No.3 gives the controller and processor of data the burden of proof by stating: "… shall be exempt from liability … if it proves that it is not in any way responsible …". As the price of non-compliance with GDPR is extremely high, organizations would need more direct guidelines of appropriate security measures. Without proper planning and guidelines explaining what appropriate security systems are needed and how to integrate them, the ambiguity could cause legal instability both for organizations and users as well.

GDPR Article 32 states three more security requirements aside from encryption and pseudonymisation. These are the ability to ensure confidentiality, integrity, availability, and resilience of the system and services, the ability to restore availability in time in case of an incident, and regular testing and assessment of the effectiveness of technical and organizational measures.

Germany

Germany, as part of the European Union, follows both national and EU legislation. One of the biggest changes that will arrive soon is the General Data Protection Regulation (GDPR, *Datensschutz-Grundverordnung[DSGVO] in German*) taking its effect in 2018. In this section, we will discuss the legal situation in Germany before and after the implementation of GDPR.

There are several laws that deal with data protection, privacy and compensation rights. The main laws that would apply to information security are the Federal Data Protection Act (*Bundesdatenschutz-gesetz[BDSG]*) and IT-Security Act (*IT-Sicherheitsgesetz*). The IT-Security Act was enacted in 2015, combining various security requirements together into one for ensuring security in German IT systems and infrastructure (BSI, "Das IT-Sicherheitsgesetz[the IT-Security Act]"). Following the IT-Security Act, the affected companies have the duty to "implement relevant State-of-the-Art (*Stand der Technik*) technical and organizational measures" to secure their services. In case of violation, the fines can go up to 100,000 EUR for critical infrastructure operators and 50,000 EUR for other services mentioned in the Act.

The "State-of-the-Art" is a term that is also used in the Federal Data Protection Act. The Federal Data Protection Act Article 9 mandates the affected parties to have a reasonable measurement taken for security, in which the official attachment to the same article states that "reasonable" is equivalent to the "State-of-the-Art." What the term entails, is not codified in the law.

Another organization, the BSI (*Bundesamt fuer Sicherheit in der Informationstechnik, Federal Agency for Security of Information Technology*) defines minimum security standards. Following BSIG Article 8, BSI is entitled to develop minimum standards for the security of information technology in Germany. Up to this point, BSI offers minimum standards aimed at federal agencies for using SSL/TLS protocols, interface control, Web browser, external Cloud services, mobile device management, High Availability Benchmarking, and are currently in the process of developing standards for shared use of external cloud services (BSI, "Mindesstandard des BSI nach § 8 Abs. 1 Satz 1 BSIG").

Challenges of data protection legislation in EU

To summarize, Germany and other European countries are showing great interest to strengthen the protection of data subjects. GDPR is bringing fines for non-compliance that are more than ten times higher than the violation of security standards of critical infrastructures. This could preclude a more security sensitive business world in Europe.

Both GDPR and national legislations of European countries, like Germany, poses vagueness utilizing the ambiguity of such terms as State-of-the-Art. State-of-the-Art is an acknowledged legal term that serves the legislators to avoid codifying a concrete technology by its name just for it to become obsolete after a few years (GDPR Report, 2017). While it still can be understood that it mostly refers to internationally or nationally well-accepted norms, such as ISO standards or BSI (*B.undesamt fuer Sicherheit in der Informationstechnik, Federal Agency for Security of Information Technology*) guidelines (Schonschek, 2016; Pohle, 2005), the complexity and vagueness is high. For example, to comprehend the State-of-the-Art for information security management systems (ISMS), one would have to work based on ISO 27001 *Information technology – Security Techniques – Information security management systems – Requirements* (Schneider). Due to the deliberate vagueness of the terms used, it is not very clear what those legal security standards include. While some minimum standards are given by the BSI in the case of Germany, first, it is aimed at federal agencies, and second, the standards are not focused on reacting to breach incidents.

GDPR mentions incident related requirements but does not define them. Breach-focused incident response planning, as well as methods to gather digital evidence, are not light topics considering the potential legal and social impact their absence could have on businesses.

South Korea

South Korea is a country that relies heavily on IT infrastructures, especially as several of the biggest South Korean companies are electronics-based, such as Samsung and LG. Consistently ranked as one of the countries with the highest average internet connection speeds, Korea is a nation in which technology is widespread and deeply integrated into society. Under these circumstances, the government also attempts to protect the infrastructure. Heavily criticized for being unprepared during data breach incidents in the past few years, South Korea has tried several approaches to promote security against intrusion.

Aside from the Personal Information Protection Act, Korea also has the Act on Promotion of Information and Communications Network Utilization and Information Protection (AICN). The latter is

lex specialise (a law governing a specific subject matter; overrides general law), while the former is general law. Therefore, regulations in AICN override the Personal Information Protection Act, should they overlap in context. The necessity of security requirements is stated in AICN Article 28, Protective Measures for Personal Information. The Article describes the duty to "follow technical and administrative measures in accordance with the guidelines prescribed by Presidential Decree". Before, it was only mandated to take technical and administrative measures, but due to constant data breaches that were caused by the poor security of organizations, legislators have acknowledged the need for a more detailed regulation. Thus, in 2004, the minimum standards of the measures were defined by guidelines, and in 2008, the Act was once again reformed to strengthen the protection of personal data. In 2012, the Korean telephone company KT was breached and leaked the personal data of 8.7 million people (Paganini, 2012). Not only was the stolen data sold to telemarketing companies, but the breach had occurred 5 months prior to detection causing public outrage. As a response to this and other breach incidents, legislators pushed higher standards such as separation of networks. Also, the Korea Internet & Security Agency (KISA) provided the Commentary to Technical and Administrative Measures of Personal Information. This commentary is not a guideline or suggestion but is legally binding as stated in Article 28 mentioned above. In case of non-compliance, it could result in criminal charges or administrative fines. If an organization does not fulfill the requirement stated in Article 28, the penalty can be up to 2 years imprisonment or a fine not exceeding 20 million KRW. Therefore, the purpose of the commentary is to bridge the gap of random interpretations and act as an administrative guide. The commentary goes over the Act on Information and Communication Network, explains the purpose of the law, and clarifies the terms and activities when needed.

Summary of the state of data protection legislation

Besides South Korea, which recently clarified their security requirements, all other countries represent dispersed, vague and law bar data protection standards.

Using the examples of several countries, we showed how the legal documents used vague definitions like "state-of-the-art" or "reasonable" in the description of security requirements. Though, these terms help documents stay up-to-date in a continuously changing technical world, they open a wide room for interpretation and consequent negligence. There are a number of lawsuits for negligence, but the current legislation handles poorly the requirements which can prevent the negligence and increase responsibility.

This section with its survey of data protection legislation in the selected countries shows the lack of effective enforcement, penalties and victim compensation (Kierkegaard, 2013). In the US, many states lack laws that allow the users to sue companies for damages related to data leaks (Kierkegaard, 2013). Even in states where data breach lawsuits are permitted, users have difficulties in proving the extent of their harm which would result in appropriate compensation. This is a common problem that victims face in other countries as well. Being unable to prove legally recognizable harm means that the relevant companies either pay too small a fine or are found not liable for compensation. This sort of low threshold for legally mandated security is problematic as companies are likely to decide to pay the fine instead of investing money and time enhancing their security.

According to a data breach litigation report in the US, the most popular legal theory used in such allegations by plaintiffs was negligence. In 2016, negligence was included in 95% of all complaints against data breaches (Bryan Cave, 2017). Most legislation that has a legal requirement of maintaining an "appropriate" level of security penalizes or imbues fines to organizations that have neglected their duty to keep the entrusted data of their clients safe. However, by many experts' standards, this legal requirement does not meet even the bare minimum level of security and does not contribute to improvements in information security in organizations.

One of the most recent cases that set a guideline of this threshold in the US was the case of the retailer corporation Target after a massive data leak in 2013. Target's security system had managed to detect the breach, but no one had understood the significance of the detection and therefore no action was taken. This resulted in over 40 million cases of compromised credit card and debit card information and over 70 million cases of personally identifiable information being stolen. The resulting settlement established security standards that Target needed to follow, but critics cannot overlook that those standards are still a basic and low bar. For example, the settlement included penetration tests and other methods to assess security measures but did not make continuous assessment necessary. Some experts expressed that "[the settlement terms] represent yesterday's security paradigm" (Rashid, 2017).

Though legislations of data protection exist, the undefined mechanisms for the quantification of the damages, minimum threshold for appropriate security and vague terms in documents cause negligence, ineffectiveness and poor adoptions of security controls in government and private companies resulting in constant and severe data breaches.

Review of initiatives in the US, EU, Germany and South Korea for the implementation of Digital Forensic Readiness

In this and following sections we analyze efforts by the selected counties to promote implementation of Digital Forensic Readiness. Section Review of initiatives in the US, EU, Germany and South Korea for the implementation of Digital Forensic Readiness, the current one, explains how the US, EU, Germany and South Korea developed non-binding guidelines and other initiatives related to DFR. Section Case study: implementation of Digital Forensic Readiness as mandatory requirement in the UK gives a case study of the UK which was the only country with the legislation of DFR.

The United States

The US has made several attempts to integrate digital forensics into information security. One of them is the "Guide to Integrating Forensic Techniques into Incident Response" published by the National Institute of Standards and Technology (NIST) (National Institute of Standards and Technology, 2006). The guide states the necessity of implementing forensic skills into incident response as it is used for diverse tasks such as operational troubleshooting, log monitoring, data recovery, data acquisition, audit purposes. In Appendix A - Recommendations, organizations are prompted to prepare a forensic capability. Forensic capability includes identifying appropriate parties for each aspect of forensics, training analysts and incident handling teams in forensic skills, establishing forensic policies and being technically prepared by using forensic toolkits. In this context, Digital Forensic Readiness can be understood as having an appropriate level of forensic capability to use digital forensic skills in case of incident handling.

Another example, the US is promoting the use of digital forensics is the Sarbanes-Oxley (SOX) Act. According to Section 404 of this act, corporations must assess how effective their internal controls are and annually report this effectiveness statement to the Security and Exchange Commission (SEC), and the assessment needs to be audited by an outside auditor. To comply with section

404, corporations need a great number of electronic records, thus making forensic analysis of those records necessary in case of incidents (The Impact of the Sarbane-Oxley Act). Section 802 forbids employees from altering or destroying records. Digital forensics could be used to prove whether there have been deliberate alterations on the files, but also corporations could use the obtained digital evidence to prove their innocence. Digital Forensic Readiness could be a helpful concept for corporations that need to manage and secure large amounts of electronic records.

Digital evidence can also be used in eDiscovery processes. eDiscovery refers to a process in litigation whereby electronically stored information (ESI) needs to be identified, collected and produced in response to a request in a lawsuit or investigation (Sedona Conference, 2010). Implementing Digital Forensic Readiness would be a good way to prepare collection and storage of digital evidence; the goal of Digital Forensic Readiness in eDiscovery would be maximizing the capability to obtain ESI that could potentially serve as digital evidence in court, while minimizing the cost that could occur in the following investigations (Sule, 2015).

As a country that supports the usage of digital evidence in legal discovery (Sammons, 2012), it can be predicted that forensic skills will have an inevitable place in information security in the future. By developing federal minimum standards and integrating Digital Forensic Readiness as one of those standards, both businesses and customers will have the privilege of improved information security.

EU and Germany

One of the big changes countries in the EU face is the stricter legislation regarding data breach notification. According to GDPR Article 33, an organization has 72 h to report an incident, which includes finding out what the breach is, what damage has been done, and how the breach has occurred. While the legislation does not directly state the technology that needs to be used, this process would most likely need extensive forensic analysis, for which Digital Forensic Readiness could help to reduce great costs by simply being prepared to gather digital evidence and perform forensic investigation. Without Digital Forensics Readiness it would be even difficult to secure the perimeter of the breach (Studio Fiorenzi Security and Forensics, 2017).

On the national level, Germany's BSI (*Bundesamt fuer Sicherheit in der Informationstechnik, Federal Agency for Security of Information Technology*) has published several non-binding guidelines that suggest integrating preparation for forensics into information security.

Last updated in May 2017, the guideline "Precautions for IT Forensics (Vorsorge fuer die IT Forensik)" acknowledges 5 stages of using forensics in IT security: (1) Strategic planning, (2) Initializing process, (3) Collecting Evidence (Live- and Post-Mortem Forensics), (4) Analysis, and (5) Reporting. The objective of this guideline is to explain what kind of precautions is needed for an efficient IT Forensics. The focus lies in preparation stages for the evidence collection stage. It sets basic requirements for the preparation of IT Forensics and lists standard requirements in compliance with the State-of-the-Art.

Another reading material BSI offers is "Guide to IT Forensics (Leitfaden IT Forensik)" (BSI, 2011). This guide, primarily targeted at IT system administrators and security personnel, shows a more detailed forensic process including two different types of Digital Forensic Readiness. One is the strategic readiness (strategische Vorbereitung), the other is the operational readiness (operationale Vorbereitung). The strategic readiness refers to preparations such as putting together a digital forensic toolkit, documentation, or setting the server to be forensic-ready, while operational readiness is the first investigative act; it serves to gauge the actual investigation area such as the breached network and identifying the data sources within. The documentation created in the strategic readiness phase helps to make work in the operational readiness faster as it provides an overview of data sources. The guide sees Digital Forensics as a way to analyze data, and help to clear the cause of breach incidents and both strategic and operational readiness is an essential part of the process.

South Korea

The financial institutions in South Korea have shown growing interest in Digital Forensic Readiness lately (Financial Security Institute (FSI), 2016). In fact, one of the major accomplishment the Financial Security Institute (FSI), a governmental body created to ensure safety and reliability in electronic financial transactions, has managed was publishing the Guideline for Incident Readiness in Financial Businesses in December 2016. While it is not legally binding, it is nevertheless important as it is the first governmental attempt to integrate Digital Forensic Readiness into the Korean IT security models. Although the title of this guide is called Incident Readiness, the term is used equal to Digital Forensic Readiness. The guide states that it has chosen that specific term to emphasize their focus on incident response instead of forensic investigation, although the terminology research used to define the term was on Digital Forensic Readiness (Financial Security Institute (FSI), 2016). The audience of this guide is financial businesses that need to prepare for investigating breach incidents. The guide is supposed to be a supplement to preserve digital evidence, conduct better investigation to guarantee business continuity. The guide explains the concept of Digital Forensic Readiness, digital evidence, and type of forensics as well as tools the businesses could use. It also provides a list of legal, technical and human resource requirements, a list of digital evidence categorized in the type of incident, OS and network, and a checklist for self-assessment of incident response readiness.

Summary of the attempts of Digital Forensic Readiness implementation

This section discovers that every country identified the importance of digital forensics and to some extent mention preparing strategically or technically to conduct a more cost-effective, successful digital investigation. Guidelines such as the German "Guide to IT Forensics" or the South Korean "Incident Readiness" actively describe how to implement Digital Forensic Readiness into organizations. For example, the "Guide to IT Forensics" explains how to operate a central log server to collect more digital evidence, while "Incident Readiness" provides a checklist about obtainable digital evidence, legal compliance and appropriate procedures for potential investigations.

The countries analyzed in this section are currently not forcing Digital Forensic Readiness as mandatory requirements. This could be due to the reluctance of organizations to invest in a preparational procedure or lack of awareness. However, this section has shown that governments are actively promoting the usage of digital forensics in organizations, have found growing interest in preserving digital evidence and consequently, suggest implementing Digital Forensic Readiness to ensure an effective digital investigation.

Next section shows a case study how the UK legislated DFR and suggests directions for the adoption of similar approaches by other countries.

Case study: implementation of Digital Forensic Readiness as mandatory requirement in the UK

Digital Forensic Readiness became a mandatory requirement in the UK. This section investigates the causes of its adoption and

analysis what it means for the improvement of security states of organizations. Along with previous sections, this section will lead into the discussion how DFR can be integrated into the legal systems of other countries and what challenges it may face. Digital Forensic Readiness is a legal requirement in the Security Policy Framework, Mandatory Requirement 37 under Security Policy No.4: Information Security and Assurance (Cabinet Office, 2010). The UK government had been discussing implementation of DFR as a mandatory requirement from the early 2000s, but after a severe data breach in 2007, the government was compelled to bring proactive forensics into their security policy.

First adopted in 2008, in 2013, the HMG Security Policy Framework underwent some changes, moving DFR requirement to mandatory requirement 9, Technical Controls (Cabinet Office, 2013). The newer version of HMG Security Policy Framework (Cabinet Office, 2014) updated a year after, seems to be the shortened, more contextual version of its previous versions.

DFR policies are not directly mentioned due to more abstract formulations of terms, but in the "Good Practice Guide (GPG) Forensic Readiness" published by the National Cyber Security Center in 2015 (National Technical Authority For Information Assurance, 2015), it is stated that the production of Digital Forensic Readiness policy is still a mandatory requirement of the Security Policy Framework (SPF MR 9). The GPG stated main reason of DFR adoption under SPF is the fact that "absence of planning increases the risk of compromise of protectively marked information" and leaves an organization more vulnerable to criminal infiltrations.

The guide aims at HMG departments and agencies to comply with SPF Mandatory Requirement 9 but recommends to other organizations as best practice. The guide devotes a whole chapter for business drivers to consider adopting a sound DFR policy. For example, regarding the costs, which causes businesses to be reluctant to implement DFR, the guide emphasizes that lack of preparation in case of an incident is likely to result in unnecessary, unorganized expenditure. Digital evidence that could serve to exempt organizations from legal liabilities could be lost and unable to be recovered, and forensic investigations would likely be handled in a disorganized manner as it will be exposed to poor governance, possibly leading to additional liabilities. On the other hand, one of the main benefits of adopting Digital Forensic Readiness is that by meshing businesses recovery plans with possible forensic investigation strategies, DFR will help to reduce business disruptions during incidents. Regarding the costs, the GPG defines different levels of DFR policies that can be adopted depending on the environmental factors of the organizations.

The legislation that mandates DFR does not list detailed requirements by name but rather uses guidelines such as GPG or samples of other policies to suggest best practices. The key findings of this implementation process can be summarized as follows:

- Digital Forensic Readiness was made mandatory for governmental organizations.
- HMG and experts have found Digital Forensic Readiness was necessary as a minimum requirement to ensure assets were managed and protected by today's IT security standards.

The SPF Mandatory Requirement 9 is only meant for governmental bodies; therefore, the HMG encourages related private sector organizations to set their security controls in line with the HMG standards by providing example policy templates. For the Digital Forensic Readiness policies to be fully integrated into the UK, it seems necessary to develop a mandating standard that also includes the private sectors.

Discussion: future directions for implementation of Digital Forensic Readiness as mandatory requirement

Is Digital Forensic Readiness needed? Should it be made a mandatory requirement?

As the summary in Table 1 shows, we observe that the private sector along with the public organizations is moving towards the proactive response to cyber threats, and Digital Forensic Readiness is an important component to achieve that goal (National Technical Authority For Information Assurance, 2015). The case study in Section Case study: implementation of Digital Forensic Readiness as mandatory requirement in the UK also shows that DFR must be made a mandatory requirement. Though it was made only a mandatory requirement for the government sector in the UK, the comparative analysis of data protection legislation in the selected countries show the necessity of strong security requirements in both public and private sectors. The vivid example of South Korea supports that statement. Our survey in section Comparative analysis of data protection legislation in the US, UK, EU and South Korea shows the vagueness and low bar of the state of security requirements in existing laws. The representative consequence of such the state is the continuous occurrence of data breaches.

The implementation of Digital Forensic Readiness will focus organizations on risk assessment and tighten security controls helping with negligence, internal and external threats (Sachowski, 2016). Careful handling of digital evidence and proactive storage of

Table 1
Comparison of government acknowledged guides for forensic readiness.

Country	United Kingdom	United States	Germany	South Korea
Mandatory	YES	NO	NO	NO
Guideline/ Best Practices	Good Practice Guide Forensic Readiness (October 2015)	NIST: Guide to Integrating Forensic Techniques into Incident Response (August 2006)	Precaution for IT- Forensics (May 2017)	Guideline for Incident Response Readiness in Financial Businesses (December 2016)
Structure and Context of Guide	-Concepts of Digital forensics -Concepts of Forensic Readiness -Risks without Forensic Readiness -Benefits with Forensic Readiness -Costs -Common Principles (comment on the principles, purpose, suggestion for adoption)	-Establishing Forensic Capability -Performing the Forensic Process (Data Collection, Examination, Analysis, Reporting) -Using the Data (text book styled guide; detailed explanations, examples) -Appendices (Recommendations, Scenarios)	-Objectives -Reference to other guides (for Detection, Incident Management, etc.) -Basic Requirement -Standard Requirement -Advanced Requirements(not state- of-the-art)	-Concept of IR readiness (focused on breach FR) -Concept of Digital Forensics -Necessity of IR readiness -IR readiness model (explains in details about forensic tools, forensic artifacts, etc.)
Checklist	YES (Capability Assessment, Forensic Readiness Policy Content)	YES (Organizing a Forensics Capability, Performing the Forensic Analysis, Scenarios)	NO	YES (Checklist for IR readiness in financial businesses)

data can solve some internal and external threats that are not only digital including fraud, HR problems, and negligence. The staff would know that organizations take data protection and security controls seriously and have substantial data.

DFR also helps during and post-incidents providing a safety net with full and admissible evidence while incident response activities may delete important data (Sachowski, 2016).

Digital Forensic Readiness is not a perfect solution. It can strengthen general security frameworks but will not be effective alone. We see challenges that some countries are still struggling with the adoption of general security requirements. So we can expect development and adoption of DFR even slower.

Another challenge is the adoption of DFR by the private sector. Private organizations are skeptical of new costs and new obligations and the only successful example of DFR as a mandatory requirement was seen in the government of the UK.

South Korea recently showed strong improvements in its legally-binding security requirements as well as initiatives towards incident response preparedness and DFR as its part for organizations other than a government, particularly the financial sector. We can expect that South Korea would implement DFR as a mandatory requirement for the private sector and would be a leading example for other countries.

As we can see pressing need for mandatory security requirements in general, growing interest to Digital Forensic Readiness in public and private sectors and an example of its successful adoption as a mandatory requirement in one of countries, we should recommend that all countries make Digital Forensic Readiness as a mandatory requirement both for government organizations and for private companies.

Conclusion

This paper has shown and analyzed the current legal situation regarding data protection law and Digital Forensic Readiness in the selected countries. All reviewed countries, while not actively trying to implement Digital Forensic Readiness models, have published guidelines to perform Digital Forensic Readiness. This is an encouraging situation, as countries in the analysis tended to have an abstract data protection law and have detailed guidelines that were binding. As for the need for Digital Forensic Readiness in these countries, it should be noted that in most, regulations for data protection were not enough for the users to receive sufficient compensation. Digital Forensic Readiness as a requirement will efficiently work as a control for information risk management and protection of personal information.

Also in the US and Germany, it could be predicted that businesses will have a growing use of digital evidence in lawsuits, making Digital Forensic Readiness preferable to implement. According to the pace of the development of security requirements in South Korea, we can expect that this country will implement Digital Forensic Readiness as a mandatory requirement.

Overall, while Digital Forensic Readiness is not yet a widely known term, countries and businesses are likely to find more use of it and follow the UK precedent to legalize Digital Forensic Readiness as a mandatory requirement.

In the dynamic technical world, we will keep monitoring legislative processes related to the implementation of security requirements. The next step will be to review adoption of GDPR in EU in 2018 and how it influenced the view of Digital Forensic Readiness. Asian countries are also rapidly developing and adopting cyber bills. Processes in China and Singapore are important to get studied.

Acknowledgements

This research was conducted as a part of the BoB (Best of the Best) cyber security education program supported by KITRI (Korea IT Research Institute).

Appendix A. Supplementary data

Supplementary data related to this article can be found at https://doi.org/10.1016/j.diin.2018.01.012.

References

Baek, S., Lim, J., 2012. A study on the forensic readiness as an effective measure for personal information protection (kor). Internet Inf. Secur. 3 (2), 34–64.
Bradford, P., Brown, M., Perdue, J., Self, B., 2004. Towards proactive computer-system forensics. In: International Conference on Information Technology: Coding and Computing.
Bryan Cave, 2017. 2017 Data Breach Litigation Report.
BSI, 2011. Leitfaden IT-forensik.
BSI, 2015. “Das IT-Sicherheitsgesetz[the IT-Security Act]”.
BSI, 2017. “Mindesstandard des BSI nach § 8 Abs. 1 Satz 1 BSIG- version 1.1.”.
Cabinet Office, 2010. HMG Security Policy Framework v.0.5.
Cabinet Office, 2013. HMG Security Policy Framework v.11.0.
Cabinet Office, 2014. HMG Security Policy Framework.
CESG, Oct 2015. Good Practice Guide No.18: Forensic Readiness. Issue No: 1.2.
Danielsson, J., Tjostheim, I., 2004. The need for a structured approach to Digital Forensic Readiness. IADIS Int. Conf. E Commer. 417–421.
District of Minnesota, March 16, 2015. In Re: Target Corporation Customer Data Security Breach Litigation. MDL No. 14–2522.
Endicott-Popovsky, B., Frincke, D.A., Taylor, C.A., May 2007. A theoretical framework for organizational network forensic readiness. J. Comput. 2 (3).
Financial Security Institute (FSI), 2016. Guideline for Incident Response Readiness in Financial Businesses (kor).
Fisher, J.A., 2013. Secure My Data or Pay the Price: Consumer Remedy for the Negligent Enablement of Data Breach. William & Mary Business Law Review.
GDPR Report, 2017. GDPR: Guidelines and Consequences for Non-Compliance. Available: https://gdpr.report/news/2017/06/16/gdpr-guidelines-consequences-non-compliance/.
Grobler, C.P., Lowrens, B., Von, Solms, 2010. A framework to guide the implementation of proactive digital forensics in organizations. In: International Conference on Availability. Reliability, and Security, pp. 677–682.
Kierkegaard, S., 2013. Data insecurity: scams, blags & scalawags. Secure Inf. Soc. 117–134.
Kosseff, J., 2017. Cybersecurity Law, pp. 65–66.
Mouhtaropoulos, A., Li, C.T., Grobler, M., 2011. Digital Forensic Readiness: an Insight into Governmental and Academic Initiatives. University of Warwick.
Mouhtaropoulos, A., Li, C.T., Grobler, M., 2014. Digital Forensic Readiness: are we there yet? J. Int. Commer. Law Technol. 9 (3).
Mullis, J., 2009. The Impact of the Sarbanes-Oxley Act of 2002 on Computer Forensic Procedures in Public Corporations. University of Oregon.
National Institute of Standards and Technology, 2006. Guide to Integrating Forensic Techniques into Incident Response.
National Technical Authority For Information Assurance, Oct 2015. Good Practice Guide Forensic Readiness. Issue No. 1.2.
Paganini, P., 2012. South Korea, Another Data Breach. How Is Changing the Hacking World? Available: http://securityaffairs.co/wordpress/7775/hacking/south-korea-data-breach-hacking.html.
Pohle, J., 2005. Persönliche Verantwortung und Haftungsrisiken von IT-Verantwortlichen – Zivilrechtliche Aspekte. DFN Arbeitstagung über Kommunikationsnetze in Düsseldorf P 73, 103–117.
Poynter, K., 2008. Review of Information Security at HM Revenue and Customs: Final Report.
Rashid, F.Y., 2017. Target's Data Breach Settlement Sets a Low Bar for Industry Security Standards. CSO. Available: https://www.csoonline.com/article/3199064/security/targets-data-breach-settlement-sets-a-low-bar-for-industry-security-standards.html.
Rossi, S., 2015. Lessons from the Target Data Breach Settlement. Law360. Available: https://www.law360.com/articles/649450/lessons-from-the-target-data-breach-settlement.
Rowlingson, R., 2004. A Ten Step Process for Forensic Readiness.
S. 1927 - Data Security Act of 2014, Section 3.
Sachowski, J., 2016. Implementing Digital Forensic Readiness – from Reactive to Proactive Process.
Sammons, J., 2012. The Basic of Digital Forensics: the Primer for Getting Started in Digital Forensics.
Schneider, T., 2017. “IT-Sicherheitsgesetz: Vage Verordnung oder konkrete Anweisung?”. IT-mod. Available: http://www.it-mod.de/it-sicherheitsgesetz-vage-verordnung-oder-konkrete-anweisung/.

Schonschek, O., 2016. Was Stand der Technik in der DSGVO bedeutet. Available: http://www.searchsecurity.de/lernprogramm/Was-Stand-der-Technik-in-der-DSGVO-bedeutet.
Sedona Conference, 2010, September. The Sedona Conference Glossary: E-Discovery & Digital Information Management, third ed. Available: http://www.thesedonaconference.org/publications_html.
Studio Fiorenzi Security & Forensics, Oct 2017. GDPR & Forensic Readiness. Available at: https://www.slideshare.net/AlessandroFiorenzi/gdpr-forensics-readiness-english.
Sule, D., 2015. Forensic Readiness and eDiscovery. Handbook of Research on Digital Crime, Cyberspace Security, and Information Assurance.
Tan, J., 2001, Technical report, @stake. Forensic Readiness.
Tsotsis, A., 2014. "Employee Data Breach the Worst Part of Sony Hack". TechCrunch. Available: https://techcrunch.com/2014/12/16/hack-sony-twice-shame-on-sony/.
Wintour, P., 2007. "Lost in the Post – 25 Million at Risk after Data Discs Go Missing", the Guardian. Available: https://www.theguardian.com/politics/2007/nov/21/immigrationpolicy.economy3.
Zurich, 2010. The Liabilities of Technology Companies for Data Breaches.