Interdisciplinary Journal of Information, Knowledge, and Management Volume 9, 2014

Cite as: Johnson, J., Lincke, S. J., Imhof, R., & Lim, C. (2014). A comparison of international information security regulations. *Interdisciplinary Journal of Information, Knowledge, and Management, 9,* 89-116. Retrieved from http://www.ijikm.org/Volume9/IJIKMv9p089-116Johnson0798.pdf

A Comparison of International Information Security Regulations

Joseph Johnson and Susan J. Lincke
University of Wisconsin-Parkside, Kenosha, WI, USA

johns369@uwp.edu lincke@uwp.edu

Ralf Imhof
Ostfalia University of Applied Science, Wolfenbüttel, Germany

r.imhof@ostfalia.de

Charles Lim
Swiss German University, Tangerang, Indonesia

charles.lim@sgu.ac.id

Abstract

Information security regulation is coming of age, with regulation very recently being passed in emerging economies. Developed nations have stable regulation, whose implementation and effectiveness can now be evaluated. This paper evaluates security regulation across both these developed and emerging economies, across four continents and six nations: China, India, Indonesia, Brazil, Germany, and the United States. We find national security regulations may be comprehensive or piecemeal; strategic or tactical in implementation; and developed in reactionary or proactive fashions.

Keywords: Information Security, International Security, Security Regulation.

Introduction

This paper evaluates how security regulation is being implemented in emerging and developed nations. Emerging market nations, such as China, India, and Indonesia, have published their information security regulation recently, while developed nations like the United States and Germany have had regulation in place for over a decade. Other countries, such as Brazil, still struggle to agree on appropriate regulation. Industry standards are also proving useful in "regulating security", particularly in nations where information security regulation is lacking, but also in all nations, where regulation may be unknown or inconsistently applied. An example of this is the Payment Card Industry Data Security Standard. This paper outlines security regulation in these nations, while briefly discussing the emerging role of the industry standard.

The need for information security regulation is substantial, since the Internet is effectively borderless, thus easily enabling international crimes and remote hacking. With over 2.7 billion people using the Internet (ITU, 2013) and

Editor: Eli Cohen

nearly 40% of the world's population, Information Security has become an international focus in this new age of computing. The Norton Cybercrime Report (2012) states that cybercrime rates are on the rise, affecting approximately 18 people every second, 1.5 million every day in the world. People are now, more than ever, falling victim to new forms of cybercrime, such as crimes found on social networking sites or mobile devices. In this paper, we will talk about how major countries, specifically China, India, Brazil, Indonesia, Germany and the United States, have responded to this increasing threat, what legislation they have passed, and problems each country is or has faced in the information security field.

Many countries in the world still are without sufficient regulation and/or enforcement to protect user's data and privacy. The highest rates of cybercrime victims are found in Russia, China, and South Africa at 92%, 84%, and 80%, respectively (Norton Cybercrime Report, 2012). The United States and the European Union have set standards for privacy and information security, which many emerging countries have used as guidelines to develop their own standards. In countries without any legislation or security guidelines set by the government, many private companies and firms look to international standards.

We are not aware of other papers devoted to this topic, which is basically a survey of international security regulation – with one exception. Many publications discuss singular security regulations. We have used some of these as our sources. Some books cover a set of security regulations for one country (notably the U.S.), but few texts cover comprehensive security for other nations. Our references were taken from four professional law journals or peer-reviewed conferences, 13 national web pages on security regulation or government reports, six news stories or blogs, seven law or security books, two dissertations on the impact of a security regulation, four security-oriented standards, and five reports published by security-oriented associations. The blog we used is published by Hunton & Williams (2013), which is a large law firm that specializes in security regulations worldwide. They have a website entitled "Global Privacy and Cybersecurity Law Updates and Analysis" where they maintain a list of recent changes in security regulations worldwide. The total number of references we have used exceed 60.

The one exception of a book dedicated to international information security is the text by Jansen, Hinzpeter, and Schwarzbart (2013): *Data Protection Laws of the World*. This text addresses the security of data in general and lacks a focus on technological or IT security. For example, the sections on the United States extensively covers electronic marketing and state breach laws, but does not address other major regulations covered in this paper, including Gramm-Leach-Bliley, Sarbannes Oxley, FISMA, FERPA, and others – although HIPAA is mentioned but not described. We use this text as one of our sources.

The goals for the paper are to answer these two questions:

1) What information security regulations exist in this country? What does the regulation address in topic and method of security implementation? How is the regulation enforced?

2) What is the environment for this regulation? How did this security regulation arise?

We interpret the topic 'Information Security' broadly, to include data privacy, computer and network security. The paper includes the following sections: regulations of emerging economies and developed nations, the emerging role of industry standards, a brief analysis of differences across all nations, and our conclusion.

Brazil

As the fifth largest country in the world with 201,009,622 citizens (July 2013 estimate), There is currently no comprehensive legislation concerning data security issues, nor any legal definitions for personal data or sensitive personal data. Privacy regulations are presently being administered by Article 5 of the 1988 Brazilian Constitution (Costa, 2012). A draft called the Brazilian Civil Rights Framework for the Internet (CRFI), also known as the Marco Civil da Internet, is a bill that has undergone considerable revisions over the past several years. The Bill is aimed to "guarantee greater freedom of expression, net neutrality, and the protection of private user data online in Brazil". The Marco Civil Bill has recently become a top priority for the Brazilian government due to recent allegations of America National Security Agency (NSA) monitoring. At this time, Brazil does not appear to restrict access to the Internet. There are also no indications that Brazilian authorities monitor e-mail accounts or Internet chat rooms.

Brazilian Constitution, 1988

Personal rights and data accuracy were finally addressed in Brazil three years after the end of a 21-year military dictatorship. Although this Constitution speaks heavily on assuring rights and liberties, it does not go so far as to lay any framework for the protection and security of data or data processing. The Constitution states that *habeas data* shall be granted to records or data banks within government or public agencies to ensure access of information and potential correction of data related to a petitioner (Costa, 2012).

Cybercrime Laws 12.735 and 12.737 (2012)

The first two cybercrime bills in Brazilian history, 12.735 and 12.737 were signed into law on Nov 30, 2012 (BKBG, 2013). Law 12.735 forces law enforcement agencies to designate special units to combat cybercrime. Law 12.737 declares the act of computer intrusions with the intent of altering, collecting, or destroying information a crime if the intruder has not received authorization from the computers owner and if the intruder violates a security mechanism. It further criminalizes any unauthorized "installation of vulnerabilities." Law 12.737 also makes distributing, selling, or producing computer programs that have this intrusion objective illegal.

The Marco Civil, Pending Litigation

The bill was first drafted in 2009 and was introduced as a piece of crowdsourced collaborative legislation. Thousands of people have since participated in public consultations online to help shape the bill's direction. The Brazilian Internet Steering Committee (2012) reports this is currently the main initiative for Internet regulation, network neutrality, privacy, internet governance and e-commerce, among other things. The bill is relevant to data protection via three aspects: risks of data leakage, the processing of sensitive data, and behavioral advertising: a way of targeting ads to users based on their habits and interests.

One major challenge with registering sizable amounts of information is the possibility of the data being "leaked" or being accidently disclosed. Without a proper management policy for such information, carelessness can lead to unintentional or even premeditated public disclosure. Episodes of leaked data have become frequent in Brazil, and public outrage has since demanded legislation to combat this. The Draft Bill addresses this problem by requiring this type of data to be handled in such a way to minimize the possibility of unauthorized access. Those who process the data are further required to utilize both technical and administrative measures appropriate to the level of technology, the specific data and type of processing, to prevent unintentional or inten-

tional disclosure or unauthorized access to personal information. The Draft Bill deems processing personal data as a risky activity, and declares that if there is an instance of leaked personal data or other property damages, the one who is directly processing the data shall be held liable.

Sensitive data processing is another topic of concern discussed in the Draft Bill. It is defined in the bill as any personal information in which the nature alone may result in prejudice towards its owner. It further delineates examples of sensitive data to include ethnic/racial information, religious, philosophical or moral beliefs, sexual preference, and personal health, genetic and biometric information. The Draft Bill forbids compulsory disclosure of such data, and also forbids the creation of a database which reveals, whether directly or indirectly, sensitive data except when permitted by express legal disposition. It further states when retaining sensitive data is acceptable, such as with the owner's consent. Sensitive data may also be retained by appropriate persons when necessary for compliance with regulation, or is within the scope of research, or if the information was previously publicized by its owner. Finally, it states that using sensitive data to discriminate against its owner is prohibited.

Behavioral advertisement is discussed as potentially having negative repercussions on consumer privacy protection. This involves, for example, placing ads on users' e-mail pages based on identifying keywords that would represent a users' interests. This practice is often viewed as invasive as it is based on gathering information from personal internet transactions. The Draft Bill proposes that personal information may only be retained with the owner's prior approval. The owner's approval must also be informed, freely obtained, and expressed. It further states that information may only be processed for its original collection intent, that of which the holder was aware of.

At the time of this writing, the Marco Civil Bill has finally been approved by the Brazilian Chamber of Deputies and is awaiting deliberation by the Federal Senate. No matter the response by the Federal Senate, it will be returned to the Brazilian Chamber of Deputies who has the final word on the legislation.

Security Practices

Data processors in Brazil are required and expected to follow reasonable measures, both technical and physical, to protect the security of personal data. However, there are currently no specific requirements or guidelines on how these security measures should be implemented. Case law requires service providers to keep access records such as IP addresses and login information for a reasonable amount of time to help identify users who may have committed crimes. Furthermore, owners of data or breached devices are not required to notify public authorities.

Enforcement

There are currently no agencies in Brazil that enforce data protection regulations, however, the passing of law 12.735 in 2012 is a historical first for Brazil in regards to combating and enforcing Cyber Crime. While there are agencies that enforce data protection, civil suits or class actions can be brought forth by either public authorities or the data subject. Jansen, Hinzpeter, & Schwarzbart (2013) reports that administrative fines can be established in amounts up to $1.5 million USD. Damage awards can reach approximately $7,500 USD for single suits or over $1 million USD for class actions.

Summary

With over 88 million internet users as of 2012 (Miniwatts, 2012), Brazil has seen its rates of internet access increase substantially over the last decade, including mobile-phone usage. However, Brazil lacks in legislation regarding what data needs to be protected as well as specifics on

how the data should be protected. The cybercrime bills 12.735 and 12.737 that were introduced in 2012 are a great starting point for Brazil and are the first laws passed specifically regarding computer crime. Brazil needs to define what they consider to be personal data and sensitive personal data, as well as specify regulations on how to protect and enforce protection for such data. The pending Marco Civil legislation, if passed, will be a significant advancement to these areas and should give Brazil their first solid framework of data protection and security regulations.

China

As the most populous country in the world with 1,356,692,576 citizens (July 2014 est.) (CIA, 2014), China (or more formally, the People's Republic of China) plays a significant role with the world's economy and society. China also has the most internet and phone users in the world as of January 2013, estimated as high as 564 million and 986 million users, respectively (Kelly, 2013). However, these users are not guaranteed the same internet freedoms and respectable levels of security as many other developed countries. The Chinese government uses enforcement techniques to govern content and institutes laws and regulations to find and punish individuals who disobey the rules.

While regulations and internet freedom have tightened recently, providing users with enhanced protection measures for personal information, by establishing laws or other tactics, has become a country-wide social concern. The Chinese government has implemented and updated much of their legislation, as recent as July 2013, to combat the ever-growing concern of cyber security and the protection of personal information. We provide an overview of the governmental agencies that are in charge of passing these laws, the legislation the currently governs the internet and information security, and outline the restrictive Internet controls used by the Chinese government to limit data content in this ever growing country.

The National People's Congress (NPC) is China's only legislative house and the largest parliament in the world, with 2,987 members. This legislative house is the only house able to pass basic laws that have nationwide application. Since the NPC only meets for roughly two weeks each year, the Standing Committee of the NPC, consisting of 150 members, meets several times a year. They also can pass national laws and amend laws passed by the full sessions of the NPC.

In 2008, the Ministry of Industry and Information Technology (MIIT) was created to develop and regulate the Internet, wireless, communications, the software industry, and other sectors of technology. They are not responsible for any type of content regulation, however.

Notice on Strengthening the Administration of Networked Smart Mobile Devices, 2013

This regulation, which takes effect November 1st, 2013, restricts manufacturers in regards to what they pre-install on smart mobile networking devices. Issued by the MIIT, the following are a few highlights of the new regulations that come at a time of rapid increase of entities manufacturing smartphones.

Without prior notice to and consent of the user, manufacturers are no longer allowed to pre-install software on smart phones that would allow the user's information to be collected or modified. This notice goes on to state that no pre-installed software can enable communication functions that could result in unfavorable results. Pre-installed software is also restricted from impacting the normal functionality of the device or the safe operation of its communication network. Furthermore, software may not incorporate data restricted by law or impact the security of the user's

personal information, network security, or legitimate interests of users. Aside from these new regulations, if any pre-installed software is added to the device or if any changes are made to the device's operating system that would affect network security, the manufacturer is required to report such changes to the MIIT.

These regulations have been introduced in response to a growing number of cases where spyware and other malicious programs have affected smart mobile devices by resulting in severe damage as well as attracted widespread attention pertaining to the risks involved with the disclosure of personal information caused by pre-installed software.

Provisions on the Protection of Personal Information of Telecommunications and Internet Users, 2013

Effective as of September 2013, these provisions, issued by the MIIT, are intended to implement a 2012 resolution on Strengthening the Protection on the Internet (detailed below) (Zhang, 2013). The provisions impose new regulations concerning the accumulation and use of personal information by telecommunication service providers as well as internet information service providers in China. These provisions mirror international data protection concepts and show motivation to implement these concepts in China.

User's personal information is defined in this provision as any information acquired during telecommunication or internet services that could identify the user when used alone or in combination with any other information. This provision imposes numerous international standard obligations regarding the gathering and usage of an individual's personal information collected during the individual's use of relevant services. Such obligations include the requirement to give notice, receive consent, limitations on collection, usage constraints, access and correction rights, what is justifiable and legal collection, and an obligation to adopt security safeguards and notification in the event that data has been breached. The provision goes on to state that penalties for violation of any of these obligations may result in administrative warning and fines.

Enhancing the protection of personal information in China has become a top priority for Chinese officials. This provision aims to improve personal information systems protection as well as clarify existing security protection measures.

Strengthening the Protection of Information on the Internet, 2012

Passed in December of 2012 by the Standing Committee of the NPC, this resolution impose requirements related to the accumulation and handling of personal information via the Internet (Zhang, 2013). The resolution characterizes information that is protected by the state as "electronic information that can distinguish the individual identities of citizens." These resolutions impose a number of requirements, most of which are directed at internet service providers (ISPs) and other organizations that process electronic personal information. Highlights are as follows:

- ISPs and similar organizations are required to embrace and adhere to rules regarding the collection and processing of electronic personal information. They must also publicize these rules.
- ISPs and similar organizations are required to identify the reason and scope of their collection and handling of electronic personal information and present it to the data subject in a clear, precise manner. They must also receive authorization from the individual whose information is being collected and used.
- ISPs and similar organizations are required to store electronic personal information using discrete, confidential means.

- ISPs and similar organizations are restricted from publicizing, changing, or sabotaging any electronic personal information that is acquired throughout the course of business activities. They are also restricted from selling the information to third parties.
- ISPs and similar organizations are required to embrace information security safeguards, and if they find users distributing information illegally, they must take immediate remedial measures. ISPs are further required to report when they find users illegally distributing information to the appropriate government agency.

This resolution further requires users to produce their true identity when agreeing to the provision of access. This part of the regulation could actually hurt the protection of personal privacy. While these regulations are fairly brief and appoint rules of very broad application, their scope is limited to Internet-related processing.

China Security Rule and Internet Censorship

Information security regulation is meant to protect organizations, the public, and the government, but anyone who uses the internet in China should also be aware of Chinese content restrictions. While China's constitution allows its citizens freedom of speech and press, Chinese laws, dating back to 1989, systematically censor content that has the potential to delegitimize the Chinese Communist Party (CCP) rule. Today, the Chinese government upholds these censorship laws by regulating not only traditional print presses, but also domestic and foreign internet sites, cell-phone text messages, chat rooms, e-mail, film, and social networking services (Wines, 2010). In April 2010, the Chinese government further changed its 1989 Law on Guarding State Secrets to enhance control on internet censorship, further restricting what the Chinese Media could report on.

Chinese authorities employ the world's most extensive content control system affecting the internet. Thousands of employees, working for both governmental agencies as well as private companies, monitor, censor, and manipulate content, including news stories and social-network sites (Kelly, 2013). This has most notably come to light when the New York Times published an article on the wealth accumulated by China's first family. Chinese authorities quickly blocked access to the New York Time's website, and reports of the news firm's computer systems being hacked surfaced shortly after.

The CCP uses three primary techniques in their content-control system: *automatic technical filtering*, *forced self-censorship by service providers*, and *proactive manipulation*.

Automated technical filtering has become known as the best layer of China's censorship system. The Golden Shield Project blocks foreign websites, by using "Web throttling" which slows down web page access to a point where the service is impractical; it can also block whole domain names or IP addresses. China Tech News (2012) reported slower broadband speeds for the month of the 2012 party congress.

The Golden Shield project, also known as "the Great Firewall," is considered to be the largest, most extensive, and most advanced Internet censorship regime in the world. By blocking foreign websites such as Twitter, Chinese authorities force their citizens to use alternative social media websites like Sina Weibo, giving them better control to censor posts.

A more common technique used by Chinese authorities is the use of deep-packet inspection technologies. This technique inspects the content requested by the user as well as its results, using a continuously evolving blacklist of keywords. If one of these blacklist words is detected, it signals technology on both ends to temporarily sever the connection. This technique is less noticeable

since the problem appears to generate from the source of information, blocking specific pages within approved sites.

Forced self-censorship by service providers places compliance with content regulations on companies. Once an international web application is blocked, it is quickly replaced by a domestic equivalent. Millions of users are attracted to these services, and as part of the company's licensing requirements, the companies are forced to guarantee that unauthorized content is not uploaded or distributed. If companies fail to take down banned content within a timely manner, they risk temporary or permanent closure (Lee, 2012). Software is usually built into the application, using blacklist databases like government inspection technologies.

Proactive manipulation, the third technique to control content, involves posting pro-government remarks in online discussions. These web commentators, hired and trained since 2005, also report users who write offensive statements or criticize government, among other things (Kelly, 2013).

Enforcement

Authorities have been granted approval to take extreme measures when punishing or stopping these unlawful behaviors. Internet service providers are also required to cooperate and provide support to supervisory authorities. There are still no enforcement regulations or legislation in regards to complying with the personal data protection requirements set forth by the PRC.

Summary

While China has very strict limitations and obstacles in regards to freedom of the internet, they have been taking large measures to secure data and place restrictions on how data can be processed. While China has a standard definition for personal data, there is currently no formal definition of "sensitive personal data" nor any proposed definition at this time. The regulations show good intent to protect personal information, but are vague in implementation: they do not specify details such as requiring risk analysis, encryption, access control or other technical requirements. Thus, it will be interesting to see how this regulation is enforced in the future.

India

While holding the second largest population in the world, with 1,236,344,631people (July 2014 est.) (CIA, 2014), India continues to struggle with development and remains a third world country. However, India's information technology industry is growing, along with an increasing number of cyber-attacks. In response, the Indian government has started implementing rules and regulations over the last few years to combat privacy issues and strengthen internet security.

The first Indian legislation was introduced in 2000, called the Information Technology Act. It was a first attempt to update obsolete laws and provide new opportunities to combat cyber-crimes. It has since been amended in 2008. Aside from these acts, many other rules and notifications have come into existence in India, many closely resembling European Standards on Information Security.

Information Technology Act, 2000

The original and first act specifically dealing with ~~i~~nformation ~~t~~echnology, this bill aimed to provide India with a legal infrastructure for e-commerce. While the act does not go into detail about Information Security or data protection, the cyber laws stated within have had an extensive impact on e-businesses and the Indian economy since their implementation, and further served as a

framework for future internet and data privacy regulations. The IT Act of 2000 also provided the legal framework for the handling and transferring of records and other various activities conveyed by digital measures. As reported by the Gazette of India (2000) the following are some of the highlights of the Act:

The first few chapters of the Act focus on digital signatures. Chapter two imposes that any user can validate an electronic record by appending their digital signature to the record. In addition, the chapter elaborates that verification of electronic records can be done by way of a public key of said user. Further chapters go onto the legal recognition of Digital Signatures, as well as detailing numerous provisions for the issuing of Digital Signature Certificates.

Chapter nine details the retribution and adjudication for numerous cyber offenses. The penalties for damage to computers and computer systems (etc.) is settled by compensating affected parties to a maximum of 1 million Rupees (or $164,370 USD). In relation, chapter 11 talks about offenses that should be investigated by law enforcement agencies. These offenses include computer hacking, tampering with computer files, or publishing obscene electronic data.

Chapter ten of the Act establishes the Cyber Regulations Appellate Tribunal. The Act further establishes the constitution of the Cyber Regulations Advisory Committee, whose goal is to provide the government advice regarding any regulations or related function connected to the Act.

While this act strongly focuses on digital signatures and penalties for cyber offenses, it does not speak specifically on information security and data protection.

IT (Amendment) Act, 2008

This amendment compliments the Information Technology Act of 2000. The Gazette of India (2009) reported that the amendment further refined the definition of information to include "data, message, text, images, sound, voice, codes, computer programs, software and databases or micro film or computer generated micro fiche". It also set out to illustrate reasonable security practices, strengthen data protection, and provide methods to keep cyber intruders at bay. The main focus of this law is to secure sensitive personal information by making the corporations that process, deal, and handle the information liable for causing unjustified loss or unjustified gain to any individual.

Information Technology Rules, 2011

Complimenting India's 2008 IT Security Act amendment, the 2011 Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules were implemented to significantly limit how businesses can handle personal information. They establish wide-ranging accountability measures for any company/organization that "collects, receives, possesses, stores, deals, or handles" personal information. The introduced accountability measures obligate companies to place restrictions on the processing of sensitive personal information and the transfer of international data, to provide privacy policies and take other security measures. Many of these new rules follow closely to the European Union protection laws, however they pose roadblocks for India's many outsourcing vendors and their clients. A summary of the new obligations follow (Gazette of India, 2011).

Restrictions on Data Collection and Processing: Companies must inform individuals that they are having their information collected at the point of initial collection. They must also be informed of the purpose the information is being collected, the designated recipients of the information, and the contact information for both the collecting agency and the receiving agency. Further, restrictions are put in place regarding the processing of the information for secondary purposes, limiting the data to be processed only for its original intent.

Definition of Personal Data: Resembling closely China's definition of personal data, India's personal data is defined as any data that relates to a natural person and is capable of identifying that individual, that may be combined with other information that a business or organization may use or obtain.

Definition of Sensitive Personal Data: Closely resembling the European Union data protection law, sensitive personal data includes information related to passwords, financial information, health information (physical, physiological, mental, medical, biometric) and sexual orientation. It further states that if the information is freely available or can be accessed via a public domain, the data is excluded from this definition.

Additional Restrictions for Sensitive Personal Data: Before sensitive data can be processed, the processor must obtain written consent from the given individual, either by letter, fax, or email.

Security: This obligation states that a corporation must comply with reasonable security practices. It further states that a corporation must document their comprehensive information security program, including policies to cover "managerial, technical, operational, and physical control measures" related to information assets and their type of industry. It also states that if an organization has a security breach, they must prove that they have fulfilled their documented security control measures. However, like Brazil, there are no established requirements to report data security breaches.

While these new rules tighten data privacy and information security, they are very broad and are not specific on how to secure information. The rules do state, however, that any organization that implements International Standard IS/ISO/IEC 27001 or an approved industry code of practice is in compliance with reasonable security practices and procedures as long as their security controls are audited annually. Further clarifications from the Indian government stated that outsourcers are Exempt from these new privacy regulations.

Future Objectives

On July 2nd, 2013, the Indian government released its ambitious National Cyber Security Policy 2013 (Ministry of Communication and IT, 2013). Of notable interest, the policy sets forth 14 diverse objectives, including development of 500,000 skilled cybersecurity professionals over the next five years. Other objectives include designating a national agency to coordinate all cybersecurity matters and the creation and operation of a National Critical Information Infrastructure Protection Center. Further objectives include enhancing global cooperation in regards to combatting cybersecurity threats and enhancing education and training programs in cybersecurity. Further objectives encourage the designation of a Chief Information Security Officer for all private and public organizations, as well as developing a dynamic legal framework to address cybersecurity concerns within areas such as cloud computing, mobile computing, and social media. These objectives are considered challenging by the Indian Minister of Communications and Information Technology Kapil Sibal, but are necessary to "ensure there is no disruption of the kind that will destabilize the economy."

Enforcement

Law enforcement agencies are encouraged under the Act to pursue cybercrimes. As required under the Act, a corporate entity is to be held liable for damages if any sensitive information that it retains, manages, or handles causes wrongful loss or gain to any individual. Civil penalties for such damages can reach up to USD $954,938 while damages paid to a civil suit may exceed this amount. Illegal disclosure of information can result in criminal fines up to USD $9,557 and/or up to 3 years imprisonment.

Summary

India has long been a country with a strong commercial background and their ecommerce industry is growing rapidly. Until recently, most of their legislation has dealt with secure business practices, however, the recent rules set out in 2011 mark a historic day for personal data protection in India. The Indian government has acknowledged that cyber security is critical to maintaining their infrastructure and their future objectives show that they are headed in the right direction.

India provides strong definitions for what they consider personal data and sensitive personal data and recent laws provide for the protection of such data. While many of the laws and regulations illustrate that personal information must be protected, there are still no laws regarding any specific technical guidelines for protecting such data. Regulations are noticeably very recent. Indian legislation has used European legislation as a beginning framework. While the resulting regulation is goal-oriented, avoiding tactical requirements, Indian law does refer to international standards as being safe implementations, when adhering to the regulation.

Indonesia

Indonesia is the largest archipelago in the world, with more than 17,500 islands that encompasses 34 provinces. Indonesia also has the world's fifth largest population, with more than 238 million people and over 668 languages and dialects. With the continuous rise of Internet subscribers in Indonesia and more than 71 million Internet subscribers in 2013, the Indonesia Internet Service Provider Association (2014) estimated the number will hit around 100 million subscribers in 2014 and around 139 million in 2015. As the number of Internet users continue to increase and in the wake of the need for law and regulation to provide data security for Internet-based electronic transactions, the Indonesian government began to establish a new cyber law in 2008.

In Indonesia, law is established to provide an umbrella to regulate certain issues in context. Subsequent government regulation is created to cover a specific issue that needed special attention. With the regulation, government or private institution in context would feel the need to comply with the established law or regulation. The laws and regulation that govern information security will provide the following benefits to business in general:

- generate new IT security-related consulting/compliance assessment jobs that would not be required otherwise;
- provide transparency to the public on whether certain business practices are in check.

Like many laws and regulation in Indonesia, sometimes they conflict with one another – they are established by different regimes sometime with different political views or will.

Since 2009, Indonesia, through the National Standardization Agency of Indonesia (2013), has established an Information Security Management Standard, which is based on ISO 27001 (SNI ISO 27001:2009). COBIT is also used to provide a mapping between the regulation and the relevant section in the standard, such as ISO and/or COBIT. The Ministry of Communication and Informatics (2013a) has been the leading government institution to take leadership in providing guidance on how to begin and measure the maturity of information security practices in the government sector that provide services to the public – Information Security Index (*Indeks Keamanan Informasi – Indeks KAMI*).

Corporations affected by information security related laws and regulation are usually banking or financial institution sectors and telecommunication sectors. The rest of the industries are usually slower in adopting this standard compared to the above two sectors. In the banking sector, Indonesia Central Bank is leading in establishing new regulation for banks in Indonesia and they are usually published as PBI (Peraturan Bank Indonesia) or Bank Indonesia Regulation (Bank Indonesia, 2013a).

PBI Number 9/15/PBI/2007

Through PBI Number 9/15/PBI/2007, Bank Indonesia (2013b) regulation mandates risk management in using Information Technology for commercial banks. While IT helps banks from an operational and customer service perspective, IT risks that could cause difficulty to the bank and its customers include operational risks and legal risks, and can also result in banking risks affecting liquidity and credit; the risk might impact a bank's reputation at the end. The latest survey by PWC (2013) showed there is a growing concern of fraud risks of banks in Indonesia including collusion between customers and employees and risk through IT platform such as e-banking, payment gateways, credit card, and debit card.

PBI Number 10/6/PBI/2008 and 6/8/PBI/2004

These Bank Indonesia (2013c) regulation, PBI Number 10/6/PBI/2008 and 6/8/PBI/2004, provides definition and explanation of implementation Real Time Gross Settlement System (RTGS) and the risks involved. RTGS is a key system to provide real time settlement between two banks that made fund transfer transactions through National Clearing System. Security and reliability are the utmost important requirement to efficient financial resources use.

PBI Number 14/2/PBI/2012 and 11/11/PBI/2009

In 2012, Bank Indonesia (BI) released Regulation No. 14/2/PBI/2012 as an Amendment to the 2009 Bank Indonesia Regulation No. 11/11/PBI, both addressing 'Card-Based Payment Instrument Activities' (*Penyelenggaraan Kegiatan Alat Pembayaran dengan Menggunakan Kartu – APMK*) (Prabowo, 2013). The Regulation mandates the precautionary principle, consumer protection, and risk management of card-based payment systems. It also regulates transaction security improvements in the form of transaction alerts to card holders; provisions on an interconnected system; outsourcing issues and emphasizes BI's authority over APMK permits and sanctions. This regulation also addresses international PCI-DSS standards for online transaction security (Prabowo, 2013). With the above regulation, credit card applicants will encounter stricter requirements, such as age limit of applicants, credit card limit and minimum income of applicant, to get their credit card approved, as publicized by Kompasiana (2012).

Law No. 11 of 2008

This Electronic Transaction Act (Republik Indonesia, 2008a) also known as the "ITE law", implements major aspects of the United Nations Commission's model law, the International Trade Law, concerning Electronic Information and Transaction. Special emphasis is placed on cybercrime and data security in Indonesia. The ITE Law requires personal consent when acquiring and using personal data via electronic media. However, the law recognizes the functional equivalence where e-transactions replace traditional transactions. This law caused much debate before passage. It has since resulted in a number of high-profile charges but also been subject to judicial review. The Ministry of Communication and Informatics (2013b) recently has planned to revise certain sections of the law abused by high ranking government officials for political reasons. To further enforce the law, Ministry of Communication and Informatics (2013c) has also recently signed a Memorandum of Understanding with the Law Enforcement Authority, i.e. Indonesia Na-

tional Police, especially in the area of cybercrime, including hacking, cracking, online credit fraud and online gambling.

Law No. 14 of 2008

With the political reform after a financial crisis in Indonesia since 1998, the Indonesia central government has since decentralized delivery of basic services to local governments through establishment of Law no 22 of 1999, as reported by United Nations Development Programme (2001). With the need for transparency, accountability and professionalism within the local governments, a new law no. 14 of 2008 (Republik Indonesia, 2008b) was established to govern public information openness. The law, also called Act of the Republic of Indonesia Number 14 of 2008, encourages public participation in the public policy making process. At the same time, the law defines information categorized as public information. Public information shall not be disclosed, if the information may impose harm to the state government, or the information may cause unfair business competition, or the information relates to privacy rights or professional secrecy, or if the requested information is not yet under control or documented.

Law No. 36 of 2009

This Law, concerned with health (Republik Indonesia, 2009), has more than 200 articles and covers many aspects of health from providers, services, and technology to data privacy of personal health information. Article 57 assures the confidentiality of personal health information managed by health care providers.

Regulation No. 82 of 2012

This regulation no 82 of 2012, on the Operation of Electronic Systems and Transactions, which enhances Law no 11 of 2008 by addressing specific issues, defines important requirements relating to electronic systems, including electronic transactions and agents, digital certifications, digital signatures and domain names. According to Robinson, Scott, and Dawborn (2013) and Republik Indonesia (2012), the Regulation applies widely to individuals, government agencies and other organizations that provide services, provide or operate e-devices, or perform electronic procedures for users with intent to prepare, process, analyze, store, display or disseminate electronic information that can be understood by any germane person. Such entities are known as "Electronic Systems Providers." Executive Director of ICT Institute in Indonesia, Heru Sutadi, mentioned in Indotelko (2013) that implementation of the law will be generally weak for 2 reasons: the law limit itself to organization that provide public service and the law also do not state specific penalties for violation of the law.

Summary

With the continuation of digitalization of information and the rapid growth of using the Internet as the means for personal, business and governmental practices, Indonesia began to enact laws and regulation, since 2007. These laws concern information security and cover electronic transactions, payment systems, and health data privacy. Some of the regulations adopt international standards such as the ISO standard and/or COBIT. Other laws or regulations are still newly established and are not specific enough in terms of coverage and details, and are subject to amendment and revision in the future to adapt to the changing needs of Indonesia. The Ministry of Communication and Informatics has been leading the effort in bringing information security practice into governmental services for the public. However, the Indonesia Central Bank is the leading organization establishing regulations for banks and other related institutions, including commercial companies, to ensure safe and secure electronic transactions that involve banks and other intermediaries.

The implementation of law and regulation in Indonesia is generally weak and it is generally due to either a lack of clear and defined penalties for violating specific laws or weak enforcement by the law enforcement officials. Government assertiveness to punish violators, which commonly involve corruption, is urgently needed. Hence, the government is now forging ahead in improving governance within its governmental institutions using continuous monitoring by the Corruption Eradication Commission. This commission was established in 2002, backed by the new law Komisi Pemberantasan Korusi (2002). Influential government officials demonstrating clean and good governance and leadership capabilities have become a theme for political figures in the upcoming general election, scheduled for April 2014. This is exemplified by one political figure, the governor of Jakarta, who acted to secure IT systems that will store the 2014 Indonesian general election information, as published in Antaranews (2014).

European Union (EU)

One of the targets of the EU is to harmonize the legal situation in the 28 Member States comprising a population of over 500 million residents. As a result, the national legislation in each of these countries is strongly influenced by EU-directives, which often provide a framework for the national legislator rather than to cause immediate effects. The legal provisions concerning IT security in Germany, the nation described next, does adhere to this European Union (EU) regulation.

In 1998 the European Union agreed to implement a Directive on Data Protection to restrict the flow of personal information within the EU member states, and to provide basic privacy rights (Stallings & Brown, 2012). These privacy rights ensure organizations secure the information, inform persons of the information they have collected, and use the information only for the purposes intended. It enables individuals to access and request correction to the data, and restrict forwarding to third parties.

Until recently, there were only a few directives dealing with the security of information technology systems. There is no detailed prescription that specifies what must be done to ensure IT security. The EU created the European Network and Information Security Agency (ENISA) in 2004, to enable an exchange of information regarding IT security matters between the Member States.

The EU regulatory framework expects telecommunication companies to perform risk management and report security incidents. In August 2013 the EU put into force a Commission Regulation ("Regulations," 2013), which pledges telephone companies and internet service providers to report data security breaches to the national authority in charge. If personal data is affected, the companies are obliged to inform their customers. The customers do not need to be informed if the data is encrypted, which renders the data unreadable. Additionally, all entities that process personal data are required by EU's data protection regulation framework to implement security measures to safeguard this data. The European Union Law (2013) also tries to establish provisions to harmonize the criminalization of specific attacks against information systems across the EU. Lastly, in January 2013, the European Union set up the European Cybercrime Center as part of the European Police Office (EUROPOL).

Since IT security in information society is crucial, the European Commission (2013) drafted a proposal for a 'CyberSec' Directive to establish measures to achieve a high level of network and information security (NIS) consistently across the EU. By this directive, the Member States shall be obliged to establish competent authorities, to whom enterprises can report security incidents. Furthermore, these authorities shall create a network to operate at the EU level. Eventually companies in specified critical sectors and public administrations will be required to perform risk analysis and act to implement sufficient and appropriate measures to assure NIS.

Germany

Germany is the nation with the highest population in the European Union, with nearly 81 million persons (CIA, 2014). It is also a major economic and political power within the EU, as well as a historic leader in technical fields: In 1936-1938, Germany's Konrad Zuse developed the first electro-mechanical binary programmable computer: the Z1. In 1970 the federal state of Hessen passed its first national data protection law.

Within Germany exists a wide range of provisions concerning IT security. In general they do not prescribe a certain specified security level but describe global targets to be reached, such as a state-of-the-art security level (Eckhardt, 2008). The most important provisions are the following, which can be classified in three groups concerning civil law, public law and criminal law.

Civil Law: German Civil Code Sec. 276 (as of 2013)

Because the Civil Law affects the relationship between legal entities, primarily it shall be up to those who establish such a relationship to determine the level of security they consider appropriate. In case an agreement on IT security is missing, Sec. 276 of the German Civil Code establishes the obligation to act with due care. In simple terms, due care means to obey the state-of-the-art level of security. Unfortunately, this level is not explicitly specified by law. Jurisdiction would refer to technical guidelines as ISO or DIN (German Institute for Standardization, a non-governmental organization) to decide whether the defendant acted sufficiently carefully. Common standards in Germany are:

- ISO 270XX (comprising a family of information security standards) (International Standards Organization [ISO], 2007);
- Evaluation of IT-products according to the Common Criteria for Information Technology Security Evaluation (CC), similar to the US Orange Book (TCSEC) (Common Criteria, 2013)

In the future, the Federal Office for Information Security (2013) (BSI) shall certify the security level of companies upon request. Today, as a service for all users of information technology, the BSI investigates IT-related security risks and provides information on uncovered threats and risks, as well as suitable IT solutions. The results of such investigations are highly esteemed by German companies at least as a basic standard of IT security.

According to German law, managers of enterprises in Germany are responsible for a high security standard for their company. Company Law obliges managers to act with the due care of a prudent and professional businessman. This covers technical measures such as firewalls, virus scanner, data encryption and data backups, as well as instructing employees to use the company's devices properly (Schultze-Melling, 2008).

Despite the high demands on IT security, there are no relevant judgments known concerning this subject. The reason for this may be that breach of IT security standards is a very delicate issue and companies do not want to clear this in public through a trial.

Public Law: Data Protection Law, 1979, 2009 and The Federal Act, 2013

Data protection provisions have the most important impact with regard to IT security. The legal basis for the security of personal information in Germany is the constitution, where it is deemed a human right. This justifies classifying the Data Protection Law as Public Law. Nevertheless it also has Civil Law aspects. Data protection is highly harmonized within the European Union, but German provisions are said to be the most demanding. Jansen, Hinzpeter, & Schwarzbart (2013)

report that the law forbids the use of personal data unless a legal exception exists or the person whose data are affected approves the use of the data.

As a reflex of the protection of personal data, every single data processor is obliged to secure the data according to specified legal rules. In particular, Section 9 of the Federal Data Protection Act, requires state-of-the-art measures be taken appropriate to the type of personal data to be secured: (Datenschutz und IT-Sicherheit, 2012).

- Authorization/Access: to prevent IT systems from being used without proper authority
- Access Control: to prevent unauthorized people from gaining access to personal data
    - to ensure that people have access only to the data for which they are authorized,
    - to safeguard that personal data cannot be read, copied, changed or deleted without authorization during processing, usage, or storage.
- Transmission Control: to ensure that personal data cannot be read, copied, changed or deleted without authorization during transmission,
    - to determine and establish where personal data may be transferred or disseminated,
- Availability Control: to protect personal data from accidental loss and destruction.

Beyond data protection, other provisions of Public Law refer to the secure storage of accounting records and business correspondence. The purpose of these provisions is that the data is accessible especially for tax administration. Technical details with respect to security levels are not technically specified.

For German Companies which are part of a group of companies, foreign law may apply as a reflex. In case the company itself or the parent company is listed in the United States, the security provisions of the Sarbanes Oxley Act (described later) must be observed.

In parallel with the legal framework for IT security agreed upon within the European Union, in March 2013 the Federal Government drafted the Federal Act to Increase the Security of IT-Systems. Companies that are important for the communication infrastructure, like telecommunication companies or huge internet platforms, shall obey state-of-the-art standards. The target is to secure information infrastructure. To determine the security level to be reached, the representatives of the telecommunications industry and the platform operators may jointly develop standards. Enterprises which realize a security breach have to report this to BSI.

Criminal Law: Criminal Code, (as of 2013)

The change towards information society revealed the importance of information and the dependency on information. As a consequence, the legislator amended some provisions to protect digital data and the security of information systems (Borges, Stuckenberg, & Wegener, 2013):

- unlawfully obtaining data for oneself or someone else that was not intended for them and is specifically protected against unauthorized access (sec 202a Criminal Code)
- unlawfully intercepting data not intended for this person or another either by technical means from a non-public IT facility or from that IT facility's transmission (sec 202b Criminal Code)
- unlawfully deleting, suppressing, rendering unusable or altering data (sec 303a Criminal Code)
- interfering with IT operations of significant importance to another by, amongst other things, "destroying, damaging, rendering unusable, removing or altering a data processing system or a data carrier" (sec 303b Criminal Code)

- deleting, suppressing, rendering unusable or altering legally pertinent data, which are not (exclusively) at this person's disposal, with an intent to cause damage (sec 271 no 2 Criminal Code)
- violation of the telecommunications secret (sec 206 Criminal Code)

Summary

While Germany is in line with the international security guidelines imposed by the EU, the EU only focuses on certain industries, such as telecom-providers or larger platforms like Facebook, Google etc. European directives do not apply to sec. 276 Civil Code or to the criminal law in general. German law refers to due care and expects state-of-the-art implementation and depends on international standards as a foundation for good security. The definition of what is state-of-the-art is very much driven by jurisdiction. Since there are no decisions defining the level of IT security in Germany, a slight uncertainty of what must be done in this context remains.

Germany distinguishes between Data Protection and IT Security. Data Protection means legal restrictions for those who (legally) possess personal data not to abuse the data by publishing it or transferring it to other people without just cause. IT Security, instead, safeguards secure information (any information, including personal data) from being accessed by unauthorized people. Data protection is very seldom subject to legal action. With respect to Germany, breaches of IT-security are not brought to court, but are instead handled privately.

United States

The United States has a total population in 2014 of approximately 319 million people, making it the fourth-most populous country in the world (after European Union and before Indonesia) (CIA, 2014). The ENIAC, recognized as the first general purpose electronic computer, was developed by the American Army during WWII in 1946. The United States invented early standards of the Internet and TCP/IP. The Internet standard evolved from ARPANET, which was first deployed in California in 1969 (Mitcham, 2005).

American information security regulation is a history of problematic crime addressed with strong compensatory regulation. Each regulation tends to specifically address committed crimes. Therefore, regulation tends to be piecemeal and non-systemic. These regulations will be addressed in historic order, with heavier emphasis on important or more computer-relevant regulations.

Family Educational Rights and Privacy Act (FERPA), 1974, and Other Student Protection Laws

FERPA protects personally identifiable information (PII) such as name, social security number, and student number (Grama, 2011). Although not listed as PII, grades are also protected. Students and their guardians at public institutions shall be able to view their records, request corrections to their records, and receive a disclosure notification annually, which tells students of their FERPA rights. Schools may disclose some defined directory information for students, but must enable students to opt out.

Other student-related regulation includes (Grama, 2011):

- Children's Online Privacy Protection Act, 1998: Protects children's privacy on the Internet, and requires parental consent before collecting personal information.
- Children's Internet Protection Act, 2000: Schools receiving federal funding must filter web content for children (e.g., pornography).

Computer Fraud and Abuse Act, 1984, and Other Computer Abuse Laws

This regulation protects against traditional cracking, including trespassing a Government or other 'protected' computer, which is any computer that participates in interstate or foreign commerce or communications (Bragg, Rhodes-Ousley, & Strassberg, 2004). The law also protects against fraud and malware. To simplify, a misdemeanor becomes a felony crime, with $5,000 damage or a threat to public safety, national security, or physical injury, or if the crime includes financial gain, commercial advantage, or criminal intent.

Related or logical extensions to this law include (Bragg, et al., 2004; Grama 2011):

- Electronic Communication Privacy Act, 1986: Disallows eavesdropping of network (felony) and stored data (misdemeanor).
- Child Protection and Obscenity Enforcement Act, 1988: Prohibits known possession of any printed, video, or digital file containing child pornography, which is transported across state lines.
- Identity Theft and Assumption Deterrence Act, 1998: Identity theft can result in 15-20 years in prison
- Anti-Cybersquatting Consumer Protection Act, 1999: Entities may sue cybersquatters, who acquire a domain name which is a registered trademark or trade name for another organization.
- Homeland Security Act, 2002: Enables the government to intercept electronic communications for national security purposes. It also makes unauthorized access to stored data a felony, when commercial gain, malicious destruction, or a criminal or tortuous act is involved.
- Controlling the Assault of Non-Solicited Pornography and Marketing, 2003: Commercial e-mailers must follow specific requirements.
- Etc.: Patent Act, 1952; Trademark Act, 1946; Copyright Act, 1976; Digital Millennium Copyright Act, 1998; Economic Espionage Act, 1996, 2012: These all deal with patents, copyright, trademarks, which are beyond the scope of this paper.

The Health Insurance Portability & Accountability Act (HIPAA), 1996

The HIPAA Act of 1996 included a Title II, which initiated a standard for the exchange of electronic health information, and regulated the protection of personal health information. This privacy protection is defined in the Privacy Rule, which protects health information whether or not it is computerized; and the Security Rule, which specifically applies to computerized health information. The original law lacked sufficient force, and thus the HITECH Act passed in 2009 to strengthen penalties, protect patients who had been harmed, require breach notification, and ensure compliance by health care providers, insurers, as well as their consultant 'Business Associates' (Kempfert & Reed, 2011). Since many businesses consult for health care organizations or maintain nurses offices, HIPAA/HITECH applies widely.

The release of personal health, addiction, or mental health information can result in social isolation, employment discrimination, and a denial of lifesaving insurance coverage. Example abuses include that a Midwest banker and county health board member, who matched customer accounts with patient information. He called due all home loans of cancer patients (Dalgleish, 2009). Blue Cross Blue Shield in Tennessee had 57 hard disks stolen, releasing medical information and social security numbers for over one million people (Dowell, 2012). Eli Lilly and Co. accidentally disclosed over 600 patient email addresses by sending one email, without blind copy, to all

registered persons who had requested reminders to take their Prozac prescription (Dalgleish, 2009).

The Privacy Rule: The Privacy Rule ensures that health care providers maintain policies regarding patient privacy, including that health information are not to be used for non-health purposes, such as marketing (Dalgleish, 2009; Kempfert & Reed, 2011). Workers shall have minimum access to patient information, sufficient only to do their jobs. Privacy safeguards should be reasonable, (e.g., privacy curtains) but not to be expensive, such as private, soundproofed rooms. Health care organizations must track both allowed and unintended disclosures of patient information. Patients have a right to obtain their patient information, request corrections, and to know who has accessed their health information, and shall receive a Notice of Privacy Practices, indicating privacy policies from their health care providers.

The Security Rule: The Security Rule recognizes that Confidentiality, Integrity, and Availability are all important in protecting Electronic Protected Health Information (Dalgleish, 2009; Kempfert & Reed, 2011). This regulation is based on risk management, to ensure that security costs correspond with risk. The goal of the regulation is that it is scalable, technology independent, and comprehensive. The regulation outlines technical, administrative, and physical security requirements, while avoiding the mention of specific technologies. Briefly, administrative requirements include risk management, alarm/log monitoring, periodic policy review/audit, and personnel management including sanction policies. Physical security requirements include a physical security plan, business continuity plans, change control, workstation acceptable use plans, and controls for devices and media (describing proper repair, disposal, and backup). Technical controls include individual authentication controls, automatic logoff/lockout, encryption and integrity controls, and event/transaction logging.

Gramm–Leach–Bliley Act (GLB), 1999

This act, also known as the Financial Services Modernization Act, applies to consumer financial transactions. It protects personal information such as: social security numbers, financial account numbers, credit card numbers, date of birth, transactions with financial institutions, and name, phone, and/or address when combined with financial account numbers (Grama, 2011).

There are three components to this regulation (Grama, 2011). The *Privacy Rule* requires that financial institutions communicate a Notice of Privacy Practices to its customers. The *Pretexting Rule* outlaws social engineering to obtain customer information, and requires that organizations include security awareness training for employees. The *Safeguards Rule* requires financial institutions develop an information security program that describes the administrative, technical, or physical controls used to protect personal financial information. This program must include a designated employee to coordinate security, a risk assessment program, control over contractors, periodic review of policies, employee training, and an incident response program.

The major problem with GLB was that it applied only to financial institutions, and not to the myriad of retailers and other companies that provide credit. Thus, its scope was too limited.

Identity Theft Red Flags Rule, 2007

A follow-up regulation to GLB, the Identity Theft Red Flags Rule, was passed in 2007 to further minimize identity theft (Grama, 2011). It applies to any creditor, including those who provide credit card accounts, utility accounts, cell phone accounts, and retailers who provide financing. These organizations must provide a written 'Identity Theft Prevention Program', which addresses for their company how Red Flags should be detected and handled by their employees. Agencies regulating this rule established five categories and 26 examples of red flag situations.

Sarbanes-Oxley (SOX) Act, 2002

During the 1990s and early 2000s, there were a number of corporations who suffered serious and highly publicized accounting fraud (Hoggins-Blake, 2009). In 2001, Enron was reported to issue statements misleading regulators and the public, and using aggressive accounting techniques in reporting profits. In 2001 and 2002, WorldCom charged expenses as capital expenses, and reported millions in profit, when they should have reported losses. Arthur Andersen LLP, an accounting and audit firm, did not follow General Accepted Accounting Practices, thereby assisting in the misleading financial reports of WorldCom, Enron, Sunbeam, and Waste Management System.

SOX passed in 2002 to protect stockholders, employees, and other stakeholders. Its general purpose is to address securities fraud, define ethics for reporting finances, increase transparency of financial reporting to stockholders and consumers, ensure disclosure of stock sales to executives, and prohibit loans to top managers. Section 404 of SOX requires that auditors newly report on internal controls, which management must certify (Ramos, 2006). Internal control is divided into Process Activity Level and Entity Level controls. Process Activity controls require the documentation of processes and transactions for specific business functional areas, and can be documented as a walkthrough for significant transactions. Entity Level controls address cross-cutting services for many business functional areas, such as IT, personnel, and risk management. Both areas address both accounting and information systems, but the Entity Level control area is most specific when addressing information systems.

ISACA's COBIT documents Section 404 requirements for information security. To establish Entity Level controls for quality and integrity of financial information (thereby minimizing fraud), the computing environment is best controlled with an implementation of IT best practices. COBIT defines best practices for the IT lifecycle: Evaluate, Direct and Monitor; Align, Plan and Organize; Build, Acquire and Implement; Deliver, Service and Support; and Monitor, Evaluate and Assess, thus deriving 37 detailed objectives (ISACA, 2012). These objectives range from "Ensure Risk Optimisation" to managing security, configuration, problems, and continuity, to "Monitor, evaluate and assess performance and conformance". This comprehensive standard defines a Process Capability Model, which enables an organization to progress to sufficiently high maturity levels.

Federal Information Security Management Act (FISMA), Part of E-Government Act, 2002

The E-Government Act of 2002 was designed to protect government information related to economic and national security interests after the September 11, 2001 terrorist attacks. Title III, FISMA, authorized the National Institute for Standards and Technology (NIST) to develop associated standards. FISMA must be adhered to by federal agencies, their contractors, and other entities whose systems interconnect with U.S. government information systems. FISMA also set in place the US-CERT, which is a national incident response center. This regulation is important, since Federal chief information officer Kundra said in 2010 that government computers are attacked millions of times each day (Grama, 2011).

The areas that FISMA addresses include (NIST, 2006): access control, security/regulation awareness and training, audit and accountability, certification, accreditation, and security assessments, configuration management, contingency planning, authentication and access control, incident response, maintenance, media protection, physical and environmental protection, security planning, personnel security, risk assessment, control of systems and services acquisition, system and communications protection, and system and information integrity.

State Breach Notification Laws, 2003 and later

Forty-six states and four territories have passed regulations requiring entities to notify persons when their personal information has been involved in a security breach (State Security Breach Notification Law, 2013). The law was first enacted in California in 2003, and enforced in 2005 when ChoicePoint learned that an identity theft ring had pretended to be customers, and possibly took personal information for over 150,000 people (Grama, 2011).

Breach notification laws apply to any entity that deals with nonpublic personal information, which includes: Social Security number, driver's license number, state identification card number, and financial account number, possibly with its access code or password. Some states may also include medical or health insurance information.

When a breach of private information is determined, the entity must notify the affected persons in a timely manner. Often, the disclosure notification must inform the victims of the breach, include the (estimated) date and nature of the breach, indicate steps the data collector plans to take or has taken regarding the breach, and may require contact information for consumer reporting agencies and/or a statement advising recommended actions. This information may be provided in written or electronic form.

In many states, stolen personal information that is encrypted is exempt from disclosure – as long as the encryption key was not also acquired. Personal information shall be disposed of in a way that ensures the personal information is undecipherable. Proper disposal methods for paper documents include redaction, burning, pulverizing, or shredding. Disposal methods for electronic and other media include destroying or erasing the media.

Civil penalties may apply in the range of $10-$2000 per affected person, with a maximum total penalty of $50,000-$150,000 per breach situation (State Security Breach Notification Law, 2013).

Summary

When security offenses are evaluated by U.S. court system, risk management weighs in heavily. Most commonly, large companies found to violate security regulation have had to pay millions of dollars to government agencies, and are often set up with a special program of remediation and monitoring for an extended period of time (e.g., CVS, ChoicePoint, TJX (Grama, 2011)). These major penalties play an important role in the risk management process, and ensure security compliance.

The current security issue, introduced by Edward Snowden's release of government data, is American and international privacy from government intrusion. The NSA has requested or manipulated companies to water down encryption algorithms; install backdoors in software products; as well as provide communication data from social networking sites (Perlroth, Larson, & Shane, 2013). This is an issue being discussed by all three branches of the U.S. government, as well as by the public and corporate America.

Analysis

We conclude that the developing nations we evaluated are addressing information security, even if their security regulations are fairly recent. This is positive, since much trade is international in scope.

One interesting comparison is the frameworks used by India, Brazil, and Germany, versus the United States. Regulations of the three former nations focus on **information** security, while the U.S. focuses on information **security**. Nations focusing on **information** security describe the information types to be protected and then state or imply that formal security standards should be

followed. When countries focus on information **security**, part of the regulation specifies the information to be protected, while the majority of the regulation focuses on the technical, administrative and physical requirements for security. For example, Germany focuses on **information** security, because the security implementation requirements are minimally specified. We conclude that the U.S. takes a tactical approach, mandating specific security implementations per industry, while Germany takes a strategic approach, assuming adherence to international standards and being non-specific about security implementations. Similarly, Indonesia refers to OSI and COBIT as international standards.

A second implementation issue is how security regulation should be enforced: according to strict standards or risk management? In the U.S., due care means that risk management has been used to ensure that security is sufficient for the job; whereas traditionally in Germany due care means implementation according to an international standard. This indicates a difference in fundamental view: in the U.S., security should be proportional to the problem/organization, with smaller companies paying less for security than bigger organizations, but with certain mandated requirements. Indonesia also mandates risk management, particularly in banking-related regulation. In Germany and India, security is guaranteed for the public, and all must meet security standards. In Europe, the approach in determining legal responsibility appears to be changing, at least for some industries. The 2013 proposed 'CyberSec' Directive, which addresses public agencies, telecommunications and other critical sectors, mandates risk management to safeguard security.

- The borderless Internet is currently causing some legal issues across nations due to cultural values. Specifically, many issues relate to different cultural and economic issues across the world. Some current issues include:
- **Surveillance State**: Snowden's releases indicate that American government spying is widespread and intrusive both within and outside the United States. Obama has admitted that government spying occurs to counter terrorism, to defend against cyber-attacks, and for national defense reasons (New York Times, 2014). China's cybertheft, directed by units of the People's Liberation Army, has used Advanced Persistent Threat methods to target intellectual property designs of many international commercial products as well as foreign government spying (Verizon 2013 Data Breach Investigations Report, 2013 and Rauscher, 2013). Other governments, including Israel, Britain, India, Russia, Brazil, North Korea, the U.S., and several Middle Eastern countries pay more than the $150,000 price that Microsoft will pay to hacker organizations per bug for zero-day attacks (Perlroth & Sanger, 2013). These cyber-spying problems threaten to restrict democracy but also reduce trust in commercial products from surveillance state nations, until the issue is resolved.
- **Internet Restrictions**: China strictly restricts criticism of the government. The U.S. restricts Internet sites that "pose an imminent threat of producing serious lawless action" (Rosen, 2012), but also collects information about personal contacts and apparently has manipulated encryption in mobile devices (Dourado, 2013). Germany and France restrict web sites featuring (among other things) holocaust denial (Rosen, 2012).
- **Privacy** or **Right to be Forgotten**: Europe and Argentina permit their people to have the ability to remove objectionable personal information from the web (Rosen, 2012). Brazil is in the process of passing the most substantial privacy regulation that protects ethnic/racial information, religious, philosophical or moral beliefs, sexual preference, and extensive health information as part of its Marco civil legislation. The U.S. believes strongly in (truthful) free speech, and tends to minimize protected information to health, financial, and identification information.

- **Copyright Materials on the Web**: Search results may point to illegally used, copyrighted, materials. Copyright owners may request that these materials not be displayed as search results. When web search engines comply, these search engines are provided a safe harbor under the U.S. Digital Millennium Copyright Act. Issues include search engines not under American control, and copyrighted images showing up in searches.

As time passes, it will be interesting to see how legal cases differ in solution based on the different approach taken.

We have also seen the increasing role of industry-oriented standards. First, many nations depend on these standards, since their regulation is non-specific, assuming adherence. Secondly, these standards become de facto law, when contracts specify adherence or companies/countries expect certification. This is particularly helpful for nations who lack security law. The most prominent and emerging industry standards include PCI-DSS (PCI, 2013), ISO 270xx (ISO, 2013), Common Criteria (2013), and Open Group (2013).

Conclusion

This paper has reviewed how information security is implemented across six nations, four continents, and in both developed and emerging economy nations. Security regulation is coming of age, but is being developed in different ways, for different reasons, and is emphasizing different focuses. We have noted that some countries' regulation refer to security goals, while others specify detailed implementations in their regulations. Some nations simply specify security goals, while others require risk management. The way nations define and protect personal privacy differs. Finally, some nations provide freer rights in use of the Internet, compared to others. These national changes are influenced by the cultural norms of the society and have different advantages and disadvantages. Organizations that span nations should not assume that security regulation in their home country applies everywhere.

Finally, it is impossible to ignore the increasing role of industry-oriented standards in 'mandating' security.

References

2012 Norton Cybercrime Report. (2012) *Norton*. Symantec. Retrieved from http://now-static.norton.com/now/en/pu/images/Promotions/2012/cybercrimeReport/2012_Norton_Cybercrime_Report_Master_FINAL_050912.pdf

Antaranews. (2014). *Jokowi siapkan tim IT proteksi hasil pemilu*. Retrieved from http://www.antaranews.com/pemilu/berita/426931/jokowi-siapka-tim-it-proteksi-hasil-pemilu

Bank Indonesia. (2013a). *Bank Regulation*s. Retrieved from http://www.bi.go.id/web/en/Peraturan/Perbankan

Bank Indonesia. (2013b). *Bank Indonesia Regulation No. 9/15/PBI/2007 - Implementation of risk management in the use of information technology by commercial banks*. Retrieved from http://www.bi.go.id/web/en/Peraturan/Perbankan/pbi_091507.htm

Bank Indonesia. (2013c). *Bank Indonesia Regulation No.10/6/PBI/2008 - Concerning the Bank Indonesia Real Time Gross Settlement System.* Retrieved from http://www.bi.go.id/web/en/Peraturan/Sistem+Pembayaran/pbi_100608.htm

BKBG. (2013, Aug. 1). *Internet Law Acts defining cybercrime offenses in Brazil are signed into law.* Retrieved from http://www.bkbg.com.br/direito-de-internet-publicadas-leis-que-tipificam-crimes-informaticos/?lang=en

Borges, G., Stuckenberg, C.-F., & Wegener, C. (2013). Bekämpfung der Computerkriminalität. *DuD – Datenschutz und Datensicherheit, 31*(4), 275 – 278.

Bragg, R., Rhodes-Ousley, M., & Strassberg, K. (2004). *Network security: The complete reference* (pp. 761-772). New York NY: McGraw-Hill/Osborne.

Brazilian Internet Steering Committee. (2012). Internet Policy Report Brazil 2011. *Observatorio Da Internet.br*. Ed. Bruno Magrani. Retrieved from http://observatoriodainternet.br/wp-content/uploads/2012/11/Internet-Policy-Report-Brazil-2011.pdf

China Tech News. (2012, November 6). In tandem with slower economy, Chinese internet users face slower internet this week. Asia Media Network. Retrieved from http://www.chinatechnews.com/2012/11/06/18835-in-tandem-with-slower-economy-chinese-internet-users-face-slower-internet-this-week

Central Intelligence Agency (CIA). (2014, April 26). *The world factbook*. Retrieved from https://www.cia.gov/library/publications/the-world-factbook/geos/in.html

Common Criteria. (2013). Retrieved from http://www.commoncriteriaportal.org/

Costa, L. (2012, June). *A brief analysis of data protection law in Brazil*. Retrieved from http://www.coe.int/t/dghl/standardsetting/dataprotection/tpd_documents/Report%20(June%204th%2012)%20-%20A%20brief%20analysis%20of%20DP%20in%20Brazil%20(updated%20version).pdf

Dalgleish, C. (2009). *HIPAA compliance*. (Course) Triton College, River Grove IL.

Datenschutz und IT-Sicherheit. (2012). *Tinnefeld, Buchner,Petri, Einführung in das Datenschutzrecht*, Oldenbourg Verlag München. 413 – 423.

Dourado, E. (2013, October 9) Let's build a more secure internet. *New York Times*. Retrieved from http://www.nytimes.com

Dowell, M. A. (2012, June). HIPAA Privacy and Security HITECH Act enforcement actions begin. *Employee Benefit Plan Review*. 9-11.

Eckhardt, J. (2008). Rechtliche Grundlagen der IT-Sicherheit. *DuD – Datenschutz und Datensicherheit, 32*(5), 330-336.

European Commission. (2013, February 7). *Proposal for a directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union.* Retrieved from http://eeas.europa.eu/policies/eu-cyber-security/cybsec_directive_en.pdf

European Union Law. (2013). Retrieved from http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0517:FIN:EN:PDF

Federal Office for Information Security [Germany]. (2013). *Taking advantage of opportunities – avoiding risks*. Retrieved from https://www.bsi.bund.de/EN/Home/home_node.html

The Gazette of India. (2000, June 9). *The Information Technology Act, 2000.* Department of Electronics and Information Technology. Retrieved from http://eprocure.gov.in/cppp/sites/default/files/eproc/itact2000.pdf

The Gazette of India. (2009, Feb. 5). *The Information Technology (Amendment) Act, 2008*. Department of Electronics and Information Technology. Retrieved from http://deity.gov.in/sites/upload_files/dit/files/downloads/itact2000/it_amendment_act2008.pdf

The Gazette of India. (2011, April 11). *Information Technology (Intermediaries Guidelines) Rules, 2011*. Department of Electronics and Information Technology. Retrieved from http://deity.gov.in/sites/upload_files/dit/files/GSR314E_10511(1).pdf

Grama, J. L. (2011). *Legal issues in information security*, Sudbury, MA: Jones & Bartlett Learning.

Hoggins-Blake, R. (2009, January). *Examining non-profit post-secondary institutions' voluntary compliance with the Sarbanes-Oxley Act*. Dissertation Submitted to Northcentral University, Prescott Valley AZ. 1-42.

Hunton & Williams LLP. (2013, May 7). Chinese Ministry issues new rule restricting pre-installation of software by manufacturers of mobile devices. Web log post. *Privacy and Information Security Law Blog*. Retrieved from http://www.huntonprivacyblog.com/2013/05/articles/chinese-ministry-issues-new-rule-restricting-pre-installation-of-software-by-manufacturers-of-mobile-devices/

Indonesia Internet Service Provider Association. (2014). Retrieved from http://www.apjii.or.id/v2/read/content/info-terkini/213/press-release-profil-terkini-internet-industri-ind.html

Indotelko. (2013). *PP PSTE Hanya Macan Ompong?* Retrieved from http://www.indotelko.com/kanal_indepth?it=PP-PSTE-Hanya-Macan-Ompong

ISACA. (2012). *COBIT5: Enabling processes*. ISACA. Retrieved from www.isaca.com

International Standards Organization (ISO). (2007). *ISO/IEC 27001:2005, Information technology -- Security techniques -- Information security management systems – Requirements.*

International Telecommunications Union (ITU). (2013). *ICT facts and figures*. Retrieved from http://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2013-e.pdf

Jansen, T., Hinzpeter, B. & Schwarzbart, P. (2013). Germany. *Data protection laws of the world.* 30, 99-104. Retrieved from http://www.dlapiper.com/files/Uploads/Documents/Data-Protection-Laws-of-the-World-Handbook-Second-Edition-2013.pdf

Kelly, S. (2013). Throttling dissent: China's new leaders refine internet control. *Freedom House*. Retrieved from http://www.freedomhouse.org/sites/default/files/resources/Throttling%20Dissent_FOTN%202013_China_0.pdf

Kempfert, A. E., & Reed, B. D. (2011, April). Health care reform in the United States: HITECH Act and HIPAA privacy, security, and enforcement issues. *FDCC Quarterly, 61*(3), 240.

Komisi Pemberantasan Korusi (2002). *Undang-Undang No. 30 Tahun 2002 Tentang Komisi Pemberantasan Tindak Pidana Korupsi*. Retrieved from http://www.kpk.go.id/images/pdf/Undang-undang/uu302002.pdf

Kompasiana (2012). *Syarat Kartu Kredit Makin Sulit*. Retrieved from http://ekonomi.kompasiana.com/moneter/2012/01/09/syarat-kartu-kredit-makin-sulit-429533.html

Lee, M. (2012, August 23). Clampdown rumored as Chinese 'twitter' sites blocked. *The Globe and Mail*. Retrieved from http://m.theglobeandmail.com

Ministry of Communication and Informatics. (2013a). Retrieved from http://publikasi.kominfo.go.id/bitstream/handle/54323613/119/Panduan%20Penerapan%20Tata%20Kelola%20KIPPP.pdf

Ministry of Communication and Informatics. (2013b). *Pemerintah Akan Revisi UU 11/2008 Tentang ITE Tahun Depan*. Retrieved from http://kominfo.go.id/index.php/content/detail/3360/Pemerintah+Akan+Revisi+UU+11-2008+Tentang+ITE+Tahun+Depan/0/berita_satker#.Uzg2NPmSx7w

Ministry of Communication and Informatics. (2013c). *Kominfo-Kapolri MoU Pengamanan dan Penegakan Hukum Bidang Kominfo*. Retrieved from http://kominfo.go.id/index.php/content/detail/1462/Kominfo-Ka-polri+MoU+Pengamanan+dan+Penegakan+Hukum+Bidang+Kominfo/0/berita_satker#.Uzg20PmSx7w

Ministry of Communication and Information Technology [India]. (2013, July 2). *Notification on national cyber security policy of information-2013* (NCSP-2013). Retrieved from http://deity.gov.in/sites/upload_files/dit/files/National%20Cyber%20Security%20Policy%20%281%29.pdf

Miniwatts Marketing Group. (2012, Nov 26). Brazil INTERNET USAGE STATS AND TELECOM MARKET REPOrts. *Internet World Stats*. Retrieved from http://www.internetworldstats.com/sa/br.htm

Mitcham, C. (Ed.). (2005). *Encyclopedia of science, technology, and ethics*. Detroit: Macmillan Reference USA.

National Institute of Standards and Technology (NIST) (USA). (2006, March). *Minimum security requirements for federal information and information systems*, FIPS Pub. 200.

National Standardization Agency of Indonesia. (2013). Retrieved from http://websisni.bsn.go.id/index.php?/sni_main/sni/detail_sni/10233

New York Times. (2014, Jan 17). Obama's speech on N.S.A. phone surveillance (Transcript), Retrieved from http://www.nytimes.com

Open Group. (2013). *Trusted tech. provider standard.* Retrieved from www.opengroup.org/news/press/open-group-releases-global-technology-supply-chain-security-standard

Payment Card Industry. (2013, June 15). PCISSC-Overview of standards. Payment card industry security standards. Retrieved from www.pcisecuritystandards.org

Perlroth, N., Larson, J. & Shane, S. (2013, September 5). NSA Able to Foil Basic Safeguards of Privacy on Web, *New York Times.* Retrieved from http://www.nytimes.com

Perlroth, N. & Sanger, D. E. (2013, July 13). Nations buying as hackers sell flaws in computer code. *New York Times*. Retrieved from http://www.nytimes.com

Prabowo, H. Y. (2012) Towards a better credit card fraud prevention strategy in Indonesia. *Journal of Money Laundering Control*, *15*(3). Emerald Insight. Retrieved from https://business.uow.edu.au/content/groups/public/@web/@commerce/@econ/documents/doc/uow120442.pdf

PWC (2013). *Indonesian Banking Survey 2013*. Retrieved from http://www.pwc.com/id/en/publications/assets/pwc-indonesia-banking-survey-2013.pdf

Ramos, M. (2006). *How to comply with Sarbanes-Oxley Section 404: Assessing the effectiveness of internal control.* Hoboken NJ: John Wiley & Sons.

Rauscher, K. (2013). Writing the rules of cyberwar. *IEEE Spectrum, 50*(12), 30-32.

Regulations. (2013). *Commission Regulation (CR 611/2013) on the measures applicable to the notification of personal data breaches*. Retrieved from http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=uriserv:OJ.L_.2013.173.01.0002.01.ENG

Republik Indonesia. (2008a). Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik. Retrieved from http://publikasi.kominfo.go.id/handle/54323613/899

Republik Indonesia. (2008b). Undang-Undang Republik Indonesia Nomor 14 Tahun 2008 Tentang Keterbukaan Informasi Publik. Retrieved from http://www.kemenag.go.id/file/dokumen/UU1408.pdf

Republik Indonesia. (2009). Undang-Undang Republik Indonesia Nomor 36 Tahun 2009 tentang Kesehatan. Retrieved from http://www.hukor.depkes.go.id/up_prod_uu/UU%20No.%2036%20Th%202009%20ttg%20Kesehatan.pdf

Republik Indonesia. (2012). Regulation of the Government of the Republic of Indonesia Number 82 Of 2012 On Electronic System and Transaction Operation. Retrieved from https://pandi.or.id/sites/default/files/u1/PP%20PSTE%20English.pdf

Robinson, M., Scott, B., & Dawborn, D. (2013). *First regulation issued under Indonesia's electronic information and transactions law.* Retrieved from http://www.lexology.com/library/detail.aspx?g=400e45ac-d9d3-4932-96fc-745acfb6dce9

Rosen, J. (2012) *Privacy, property, and free speech: Law and the constitution in the 21st century*, Chantilly VA: The Great Courses. 171-186.

Schultze-Melling, J. (2008). IT-compliance: Challenges in a globalized world. *Computer Law Review International, 5*, 142-147.

Stallings, W. & Brown, L. (2012). *Computer security: Principles and practice* (2nd ed.). Cranberry NJ: Pearson Education. 605-606.

State Security Breach Notification Laws. (2013). National Conference of State Legislatures. Retrieved from http://www.ncsl.org/issues-research/telecom/security-breach-notification-laws.aspx

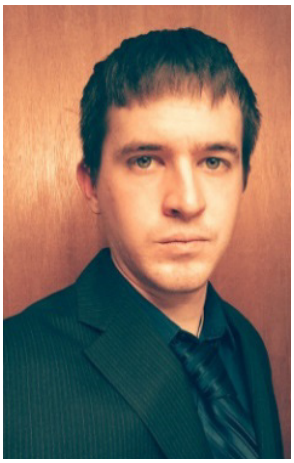
United Nations Development Programme (2001). Introducing Good Local Governance - The Indonesian Experience. Retrieved from http://www.undp.or.id/programme/governance/intro_glg.pdf

Verizon 2013 Data Breach Investigations Report. (2013). Retrieved from www.verizonenterprise.com/DBIR/2013

Wines, M. (2010, April 7). China's censors tackle and trip over the internet. *The New York Times*. Retrieved from http://www.nytimes.com

Zhang, L. (2013, January 4). China: NPC decision on network information protection. *Library of Congress*. USA.gov. Retrieved from http://www.loc.gov/lawweb/servlet/lloc_news?disp3_l205403445_text

Biographies



Joseph Johnson graduates with a double major in Computer Science and Criminal Justice from University of Wisconsin- Parkside, expected in May 2014. His interests lie in cyber and information security. He is currently employed by Wal-Mart Stores, Inc. in asset protection.

Susan Lincke PHD CISA is an Associate Professor of Computer Science at University of Wisconsin-Parkside. Her MS and PHD in Computer Science are from the Illinois Institute of Technology. She spent 17 years in software development and project management in the telecommunications industry, including working at GE, MCI, and Motorola, before embarking on her PHD and teaching. Her research is in information security planning, wireless network modeling/simulation, and service learning. Her most recent project was a NSF CCLI grant, "Information Security: Audit, Case Study, and Service Learning."

Following a two year apprenticeship with Deutsche Bank in banking, **Ralf Imhof** started his studies of law in 1986 at the universities of Bonn and Munich. During his legal internship he worked at the legal department of Deutsche Bank Argentina in Buenos Aires. Then he studied for a doctorate in Law and began working as an attorney in 1996; since 1999 with the law firm SCHULZ NOACK BÄRWINKEL in Hamburg. He became partner in 2004 and is now Of Counsel to the firm. He is appointed as a professor at Brunswick European Law School, faculty of law of Ostfalia University in Wolfenbüttel, Germany. Mr. Imhof specializes in Information Technology Law.

Charles Lim is lecturer and researcher of Swiss German University. He completed his Master Degree in Electrical Engineering from University of Hawaii-Manoa, HI, USA in 1991 and Bachelor Degree in Electrical Engineering from University of Wisconsin-Madison, WI, USA in 1989. He has extensive IT consulting experiences before joining Swiss German University in 2007. He is currently pursuing his doctoral study in Universitas Indonesia and his current research interests are Malware, Web Security, Vulnerability Analysis, Digital Forensics, Intrusion Detection, and Cloud Security. He is currently leading Indonesia Chapter of Honeynet Project and also a member of Indonesia Academy Computer Security Incident Response Team.