Does Legal Protection from Host-countries Mitigates Information Security Risk in Multinational Enterprise Subsidiaries

Full Paper

Hong Chen
Old Dominion University
hchen001@odu.edu

Yong Chen
Old Dominion University
y7@odu.edu

Abstract

Subsidiaries of multinational enterprises (MNEs) are vulnerable to cyber-attacks because they operate in diverse environments that are different from the contexts in the home countries. After they get legitimacy in the host countries, subsidiaries not only receive isomorphic pressure, but also gain protection from the local institutional environments, specifically legal protection. In recent years, information security breaches perpetrated by insiders become more common among MNEs. Directed by the General Deterrence Theory, this paper explores whether the legal protection in host-countries deters employees' information leaking behavior in MNE subsidiaries. In particular, this paper proposes that the rule of law and the efficiency of the judicial system in a host-country negatively influence MNE subsidiaries' employees' information leaking behaviors. In terms of law original, this paper proposes that MNE subsidiaries located in common-law countries experience fewer information security breaches than those located in civil-law countries. In addition, this paper argues that the level of income in a host-country is negatively related with the amount of information security breaches that MNE subsidiaries experience.

Keywords

Information security, cybersecurity, institutional theory, deterrence

Introduction

Information systems have been adopted widely by multinational enterprises (MNEs) to enhance business operations, to facilitate management decision-making, and to deploy business strategies (Kankanhalli, Teo, Tan, & Wei, 2003). As a increasing variety of transactions involving the trading of goods and services are accomplished electronically, abundant opportunities for unauthorized access to IS are presented as well (Brooks, Warren, & Hutchinson, 2002; Gupta & Hammond, 2005). For MNEs, the prevalence of offshore outsourcing and other managed data services has introduced significant information security problems (Hovav & D'Arcy, 2012). In a 2006 survey that examined the privacy policies of 47 U.S. and E.U. multinational companies, 94 percent of the E.U. companies reported that they had experienced an information security breach (ISB) during the past three years, compared with 86 percent of their American counterparts (Cline, 2006). ISBs are big threats for MNEs because such intrusions increase their expenses, decrease their profits and dividends, drop their stock prices, damage customer confidence, and reduce market values (Power, 2003). Once ISBs occur, huge number of customers can be affected. For example, in 2011, Sony experienced an ISB that led to a leak of 77-million users' account information (Reuters, 2011). Moreover, ISBs could cause tremendous financial losses as well. The average cost of an ISB for a U.S. corporation during the first quarter of 2012 was estimated to be $4,688,139 (Visser, Hardin, Drage, Pinne, & Drage, 2012).

According to Symantec (2012), although the main threats for IS systems are from malicious outsiders (hackers), insider threats caused by employees' intentional and unintentional leaking or stealing of valuable data have been increasing in recent years. MNEs have spent millions of dollars on technology to

prevent outside attacks. Their technology, however, has not able to prevent insiders from disabling it or doing unintentional damage (VanCura, 2005). The most frequent cause of ISBs was theft or loss of computers or memory sticks on which data is stored or transmitted (Symantec, 2012). Meanwhile, another survey from Computer Security Institute (2011) indicates that nearly half of significant security breaches are perpetrated by malicious and/or non-malicious insiders.

As ISB reports have continued to rise in recent years (Richardson, 2009), information security attracts continued attention from practitioners and scholars. The ISB literature has been focused on deterrence (Hovav & D'Arcy 2012; Kankanhalli, Teo, Tan, & Wei, 2003), information security policy enforcement (Yayla, 2011), top management support (Knapp, Marshall, Rainer, & Ford, 2006), security breach notices (Cate, 2008), and trust (Al-Awadi & Renaud, 2007; Dols & Silvius, 2010). ISBs occur when information system security measures are not effective and unauthorized persons take advantage of that ineffectiveness. The effectiveness of information system security measures depends on the kind of deterrence that can dissuade potential abusers from criminal behavior through fear of sanctions (Forcht, 1994). Williams and Hawkins (1986) point out that sanctions are effective when people feel that they will definitely be punished for what they did and know that the punishment will be harsh. Therefore, deterrence relies on the certainty of sanctions and the severity of sanctions (Blumstein, 1978).

When MNEs span multiple continents, their subsidiaries face specific challenges in maintaining their information security because they operate in diverse environments that are different from the contexts within their home countries. For them, deterrence about information security on their employee, at the country level, mainly stems from the overall development of the jurisdiction's legal systems in the host countries and the effectiveness of their judiciaries, more specifically (Kaufmann, Kraay, & Mastruzzi, 2009; Djankov, La Porta, Lopez-de-Silanes, & Shleifer, 2003). In other words, MNE subsidiaries' information security relies on protection from the formal institutions (North, 1990) or the regulative pillar (Scott, 2001) in the host countries. Therefore, host countries' institutional environments, specifically the legal aspects of those institutional environments, should not be ignored when studying MNE subsidiaries' information security.

Prior research has explored the impacts of host countries' institutional factors on MNE across border expansions, such as joint venture partner selection (Roy & Oliver, 2009), entry mode (Brouthers, 2002; Delios & Henisz, 2003), investments in host countries (Globerman & Shapior, 2003; Holburn & Zelner, 2010), and subsidiaries' human resource management practices (Björkman, Fey, & Park, 2007). The focus of prior research is how MNEs gain legitimacy in host countries by adapting their strategies and operations to the local institutional environments. However, it is not noted that that MNE subsidiaries receive protection from local legal systems, once their legitimacy is determined. In terms of information security, MNE subsidiaries benefit from the deterrence generated by the legal systems in their host countries. Although Yayla (2011) argues that high institutional distance between a parent company and its subsidiaries has a negative effect on the process of enforcing information security policies to the subsidiary, the question that remains unanswered is: How do host-country legal environments influence MNE subsidiaries' information security? This paper aims to explore this question and to make contributions to improving information security for MNE subsidiaries.

This paper predicts that a host country's legal environment, its rule of law, and the efficiency of its judicial system will negatively influence MNE subsidiaries' information security, and in particular will influence the number of their ISBs. It theorizes that the host countries' legal environments are a factor in MNE subsidiaries' ISBs because they provide the rules of the game within which employees in MNE subsidiaries follow the information security regulations and generate deterrence that dissuades employees from abusing information. In addition, this paper argues that the extent of ISBs experienced by MNE subsidiaries is impacted by the host countries' origin of law and level of income. The contribution of this paper is that it applies institutional theory to MNE subsidiaries' information security, thereby providing information security literature with novel underpinnings.

Literature Review

Information Security Breach

An information system is "any combination of information technology and people's activities using that technology to support operations, management, and decision-making" (Ellison & Moore, 2003:67). To

enhance their business operations and to add to their strategic advantages, MNEs have become increasingly dependent on information systems. As the business environment becomes more electronically interconnected, information security concerns become paramount (Kankanhalli, Teo, Tan, & Wei, 2003). When handling information, MNEs need to identify and minimize risks in order to preserve the confidentiality, integrity, and availability of their information (Pelaez, 2010). An information security breach (ISB) is defined by most breach laws as "unauthorized access to defined categories of personal information" (Cate, 2008:4). An ISB can result from "loss or theft of data or equipment on which data is stored", "equipment failure", "human error", or even "unforeseen circumstances such as a fire or flood." (Information Commissioner's Office, 2008). According to Cate (2008), ISBs occur not only when specific information has been accessed without authorization, but also when such information is lost or stolen, even though it has not been accessed. Information system security handles "the prevention, detection and response to adversaries' attacks, and recovery from successful attacks." It involves "procedural and administrative processes that are implemented in order to protect information systems" (Chaula, 2006:17).

For MNEs, an ISB usually entails huge financial penalties, expensive lawsuits, and loss of reputation and businesses (Mishra, 2011). The extent of ISBs indicates how severe the results caused by them can be. The extent of an ISB is usually measured by the types of data that are exposed, the financial losses, and the total number of ISBs during a specific period (Computer Security Institute, 2011; Visser, Hardin, Drage, Pinne, & Drage, 2012). Very often, customers' personal information (e.g., name, social security number, phone number, email, and medical record) and/or financial information (e.g., credit card number) are exposed when ISBs occur (Visser, Hardin, Drage, Pinne, & Drage, 2012). The data types mentioned above can somehow indicate the range of the effect caused by ISBs. When calculating financial losses, both direct losses and indirect losses are calculated. The former, which includes the cost of responding to the incident, hiring investigators, and sending out notification letters etc., is easy to calculate, whereas the latter, which includes the losses of customers, future business, and capital etc., is harder to measure (Computer Security Institute, 2011). The combination of these three measurements, namely data types, financial losses, and total number of ISBs, might be an effective method to gauge the extent of MNEs' ISBs during a given time period.

ISBs occur when information system security measures are not effective and unauthorized persons take advantage of that ineffectiveness. Information system security effectiveness is the ability of information system security measures to protect against the unauthorized and deliberate misuse of the assets of the local organizational information system by individuals, including violations against hardware, programs, data, and computer service (Straub & Welke, 1998). Factors such as information security policies, industry type, top management support, firm size, deterrent efforts, and preventive measures, affect information system security effectiveness (Dhillon & Torkzadeh, 2006; Kankanhalli, Teo, Tan, & Wei, 2003).

Identifying where information abusers come from is critical for improving information system security effectiveness, specifically for MNE subsidiaries, which often spread around the world. According to the Computer Security Institute (2011), nearly half of significant ISBs are perpetrated by malicious and/or non-malicious insiders. McAfee (2005) reveals that company insiders mainly misuse information by: (1) allowing family and friends to use company laptops and personal computers for internet access; (2) connecting personal devices to company computers; (3) Storing personal content on company computers; and (4) downloading prohibited content at work. Many technological and/or policy measures targeting at insiders can be taken to improve MNE subsidiaries' information security. This paper, however, focuses on exploring how deterrence from legal systems at the country level in host countries affects MNE subsidiaries' information system security effectiveness.

Deterrence and Formal Institutions

General deterrence theory (GDT), a theory used in criminal justice, has been adopted by information system security scholars to explain how security countermeasures can increase the perceptions of members in an organization regarding the severity and certainty of punishment for any misuse of information (Straub, 1990). GDT is grounded in the assumption that potential criminals are rational actors. Carlsmith, Darley, and Robinson (2002) argue that deterrence makes criminal activities unattractive by changing the costs and benefits of a situation. Bentham (1962) notes that "if the apparent

magnitude, or rather value of [the] pain be greater than the apparent magnitude or value of the pleasure or good he expects to be the consequence of the act, he will be absolutely prevented from performing it" (p. 396). According to GDT, deterrent measures can dissuade people from performing certain behaviors through fear of sanctions (Forcht, 1994). Usually, deterrent measures take the form of policies, regulations, or briefings. Valid deterrent measures can make potential violators realize the certainty of sanctions and the severity of sanctions (Blumstein, 1978). Thus, effective deterrent measures are the premise of deterrence. Straub (1990) notes that deterrent measures for information security include policy statements and guidelines on the legitimate use of IS assets, security briefings on the consequences of the illegitimate use of IS assets, and audits on the use of IS assets. Their main goal is to convince outsiders and insiders who plan to perpetrate ISBs that the probability of getting caught is high and that the punishment is severe. Previous research has proven that deterrence can prevent information abuses to some extent (Straub, 1990).

At the country level, deterrence stems from laws, regulations, and rules, which are formal institutions created and enforced by a country to sanction individual or corporate actions through attaching rewards or punishments to alternative courses of behavior (Goodin, 1996). Formal institutions, together with informal institutions such as norms, cultures, and ethics, act as the "rules of the game" in a society (North, 1990). The country-level institutional factors define what is socially or legally appropriate in institutional settings (Scott, 2001) and condition firm strategies, practices, and their outcomes (van Essen, Heugens, Otten, & van Oosterhout, 2012). The institutional context of a host country is a key factor that influences MNEs' decisions and behaviors. Prior research has demonstrated the power of the host-country's institutional environment in shaping how MNEs choose an entry mode (Brouthers, 2002; Delios & Henisz, 2003), perform human resource management (Bjorkman, Fey, & Park, 2007), and select international joint venture partners (Roy & Oliver, 2009).

It is well recognized that MNE subsidiaries located in host countries are influenced by potentially contradictory pulls from the institutional factors in their local environments (Rosenzweig & Singh, 1991; Westney, 1993; Bjorkman, Fey, & Park, 2007). In a host-country institutional environment, formal institutions provide an incentive structure within which "firms rationally pursue their interests and make choices" (Peng & Khoury, 2008:260). The constraints and forces in the local environment converge and create isomorphisms, specifically coercive isomorphism, mimetic isomorphism, and normative isomorphism (DiMaggio & Powell, 1983). When MNEs span multiple continents, their subsidiaries attempt to acquire legitimacy and recognition by adopting those structures and practices that are viewed as appropriate within their local environments (Bjorkman, Fey, & Park, 2007). Coercive isomorphism coming from the rule of law and the efficiency of the judicial system in a host country forces MNE subsidiaries to adapt their strategies accordingly for survival and success (DiMaggio & Powell, 1983; Roy & Oliver, 2009). Meanwhile, it should not be ignored that when they follow the isomorphic pressure in their local environments, MNE subsidiaries benefit from their local legitimacy as well. Once they achieve legitimacy in a host country, they begin to receive protection from the local legal system. On one hand, the deterrence generated by local legal systems can prevent potential information abuses on MNE subsidiaries. On the other hand, information abusers will be caught and punished.

In their analysis of the laws in 49 countries, La Porta, Lopez-de-Silanes, Shleifer, and Vishny (1998) found that laws and the quality of law enforcement vary across the globe. They also found that the origin of law and the gross national product (GNP) per capita level in a country can affect the protection of laws. Regarding information security protection, the quality of legal rules and the process by which a judicial system handles information abusers impact the effectiveness of deterrence on information security. As such, this paper predicts that the formal institutions, specifically the legal environments, in host countries will affect MNE subsidiaries' IS security, since better institutional safeguards can prevent IS security breaches.

Theory and Propositions

Deterrence stemming from the laws, regulations, and rules in their host countries plays a key role in preventing information abuses in MNE subsidiaries. At the country level, the effects of deterrence depend on rule of law and the efficiency of judicial system (Djankov et al., 2003; Kaufmann, Kraay, & Mastruzzi, 2009). A novel conceptual model has been developed to explain how the legal environment in host countries, the rule of law, the efficiency of judicial system, and the origin of law more specifically, as well

as the level of income, may influence MNE subsidiaries' information security. Each of the model's components and relationships is illustrated in Figure 1 and each is discussed below.

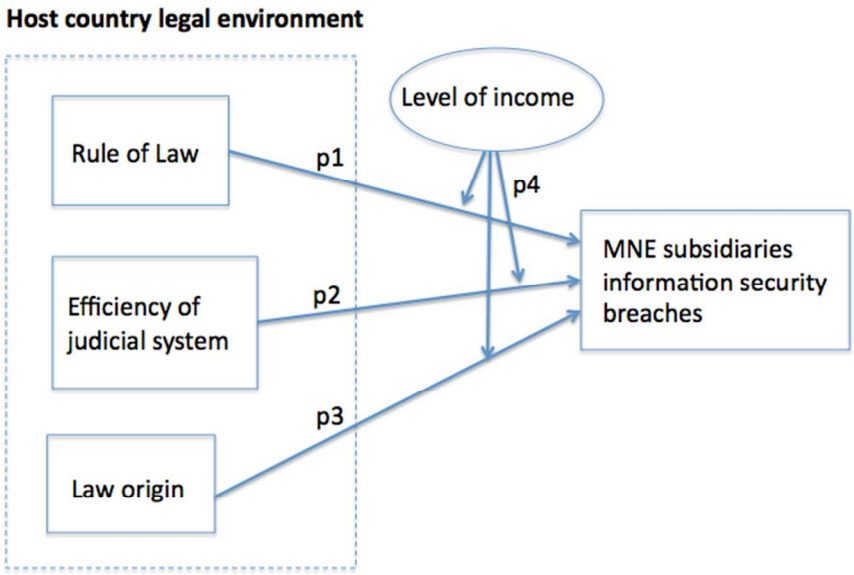

Figure 1. Host country legal environment and MNE subsidiaries information security breaches

Rule of Law

Rule of law is "a system in which the laws are public knowledge, are clear in meaning, and apply equally to everyone" (Carothers, 1998:96). It refers to "the success of a society in creating an environment in which fair and predictable rules form the basis for economic and social interactions, and, importantly, the extent to which property rights are enforced" (Cuervo-Cazurra & Mehmet Genc, 2008: 965). Rule of law requires that "laws must be open, clear, coherent, prospective, and stable, that "legislation and executive action should be governed by laws with those characteristics", and that "there must be courts that impose the rule of law" (Endicott, 1999:1). It aims to protect legal entitlements, including ownership in tangible and intangible property and personal safety (Licht, Goldschmidt, & Schwartz, 2007). It is a safeguard against arbitrary rulings in individual cases and determines the probability that those who commit crimes will be apprehended (Becker, 1968).

Rule of law varies considerably across countries. In those countries whose legal systems consist of voids, laws are ambiguous, incomplete, and contradictory (Li & Filer, 2007; Park & Luo, 2001). In addition, laws and regulations in emerging countries are usually not precisely codified (Boisot & Child, 1996; Peng &Zhou, 2005) and they tend to be complex and unstable (Doh & Pearce, 2004; Peng & Zhou, 2005). These characteristics damage the rule of law in these countries. Strong rule of law provides clear guidelines for individuals about which behaviors are allowed and which are not. By maintaining law and order well and by punishing crimes, a strong rule of law can generate an effective deterrence. By contrast, a legal environment with a weak rule of law is ambiguous, contested, and riddled with loopholes (Scholz, 1984). The lack of clear guidelines can make individuals feel confused about their behaviors. In this case, the effectiveness of the deterrence is in question due to lacking premise.

Since it is an intangible property, information relies on laws for protection. A strong rule of law regarding information security in a host country can generate effective deterrence, which can protect MNE subsidiaries from suffering ISBs. Deterrence works during the process when potential information

abusers calculate the costs and benefits of their actions. When clear guidelines are available, potential information abusers (insiders in this case) can clearly compare the costs and benefits before abusing any information. On the contrary, a weak rule of law cannot generate such strong deterrence to prevent ISBs. Consequently, this paper conjectures a negative relationship between the rule of law in a host country and the number of the country's MNE subsidiaries' ISBs. This leads to the following proposition:

Proposition 1. *The rule of law in a host country negatively influences the extent of the information security breaches that multinational enterprise subsidiaries operating in this country experience.*

Efficiency of Judicial System

Laws do not have any effect if they merely stay on the books. In order to have an effect, they must be applied by their judicial systems. Laws vary across countries; different countries enforce laws to differing extents, depending on the efficiency and honesty of their judiciaries (Jappelli, Pagano, & Binco, 2005). Judicial systems that lack properly developed court systems, arbitration institutions, and legal consultancies are not efficient (Delios & Henisz, 2000; Peng & Heath, 1996). A transparent and efficient court system is likely to provide better protection in information security, whereas poor judicial enforcement will increase opportunistic behavior, and it can be anticipated that information abuses will be more likely to happen (Jappelli, Pagano, & Binco, 2005). Luo (2007) also argues that perception of law unenforceability in a country increases the incidence of opportunistic behavior. When opportunistic behaviors are not punished, the effect of any deterrence is in question. As Williams and Hawkins (1986) point out, deterrence occurs when individuals realize that they will definitely be punished for what they did and that the punishment will be harsh.

In term of information security, a highly efficient judicial system ensures that information abusers will be punished and that the the punishment will be harsh. Effective deterrence is generated in this way because possible perpetrators will be dissuaded from opportunistic behaviors. Potential information abusers will have to consider the costs before they abuse information. In contrast, a less efficient judicial system cannot guarantee that information abusers will get harsh punishments. As a result, deterrence will not be strong enough to dissuade opportunistic behaviors regarding information security. Therefore, this paper posits a negative relationship between the efficiency of the judicial system in a host country and the number of its MNE subsidiaries' ISBs. This leads to the following proposition:

Proposition 2. *The efficiency of the judicial system in a host country negatively influences the extent of information security breaches that multinational enterprise subsidiaries operating in this country experience.*

Law Origin

Although laws vary a lot across the world, they mainly come from two broad traditions: common law and civil law (La Porta et al., 1998). La Porta et al. (1998) note that common law originates in English law, which allows judges to resolve specific disputes, whereas civil law derives from Roman law and uses statutes and comprehensive codes as a primary means of ordering legal material. Civil law relies heavily on legal scholars to ascertain and formulate its rules (Merryman, 1969). La Porta et al. (1998) argue that common-law countries give shareholders and creditors stronger protection than civil-law countries do. As such, this paper posits that MNE subsidiaries operating in common-law countries are afforded stronger protection than those in civil-law countries. This leads to the following proposition:

Proposition 3. *Multinational enterprise subsidiaries operating in common-law countries have fewer information security breaches than those operating in civil-law countries.*

Level of Income as a Moderator

It is generally thought that strong law enforcement can compensate for the quality of laws in countries with poor laws. But La Porta et al. (1998) argue that the quality of laws cannot be substituted for or compensated for in this way. They point out that the quality of law enforcement improves sharply with the level of income. They argue that the level of per capita income of a country has an important confounding effect on law enforcement. They further argue that richer countries have higher quality law enforcement, and that the quality of law enforcement is the highest in the Scandinavian and German-civil-law countries and the lowest in the French-civil-law countries. A high quality of law enforcement allows countries to fight crimes more effectively and generates better deterrence than a low quality one. Given the impact of the level of income on the quality of law enforcement, this paper conjectures that MNE subsidiaries operating in countries with a high level of income experience fewer ISBs than those in countries with a low level of income. This leads to the following proposition:

Proposition 4. *All other things being equal, MNE subsidiaries experience fewer information security breaches in host countries with higher levels of income.*

Discussion and Conclusion

MNEs must take into account the institutional factors in host countries when they span their business across continents. The isomorphic pressure coming from the local institutional environment pushes the subsidiaries to get legitimacy in host countries. However, it should not be overlooked that once MNE subsidiaries achieve legitimacy in host countries, they are covered by the protection of the local institutional environment, especially the legal environment. This protection is vital for MNE subsidiaries' information security because the number of ISBs perpetrated by insiders has been increasing in recent years. Deterrence stemming from the rule of law and the judicial system in local legal environment can stop information abuses by indicating to potential information abusers the costs and benefits of their behaviors. Just as laws and law enforcement vary across countries, differences in the effect of deterrence exist among countries. Therefore, this paper argues that the effect of deterrence is negatively related with the number of the MNE subsidiaries' ISBs. More specifically, the rule of law and the efficiency of the judicial system in a host country negatively influence the number of MNE subsidiaries' ISBs. Furthermore, this paper argues that the origin of law and the level of income in a host country impact the number of MNE subsidiaries' information security breaches. This paper extends the research of the impact of the host country's institutional factors on MNE subsidiaries by taking considering the protection that MNE subsidiaries receive from local legal environments, once their legitimacy is established. This paper offers MNE managers an institutional perspective, considering the legal environment more specifically, about how to minimize ISBs and improve information security. Managers in MNE subsidiaries can take advantage of the protection from their local legal environments and can improve their information security effectiveness.

In addition to the aforementioned contributions, this paper has the following limitations. First, although recent data show that information security threats from insiders have been increasing and remain high, threats from outsiders still exist and account for some proportion of ISBs. For MNE subsidiaries, potential outside hackers are not limited to placement within the borders of host countries because of the wide spread of electronic transactions, based on the Internet. Deterrence generated by the laws one of a country works on insider breachers, but those laws do not span across borders. Future research needs to explore how local legal environments in host countries can impact the number of ISBs committed by outsiders. Second, Phillips and Votey (1972) point out that deterrence stems from resources, such as the law enforcement system, the judicial system, and the correction system. This paper takes into account the judicial system and law enforcement, but neglects the correction system. Future studies on how the correction system in a host country impacts deterrence and further influences MNE subsidiaries' information security are needed.

A challenge for future studies is to get ISB data. Companies are extremely unwilling to admit when they have an ISB, simply because they do not want consumers to lose faith in them. This desire to keep

problems secret makes it very hard for researchers to collect data about the frequency and the number of losses due to breaches in information security (Barker, 2003).

REFERENCES

Al Awadi, M., and Renaud, K. 2007. "Success Factors in Information Security Implementation in Organizations," in *Proceedings of the IADIS International Conference e-Society 2007. Lisbon, Portugal*.

Barker, C. 2003. "Ghosts in the Machine: The Who, Why and How of Attacks on Information Security," http://www.sans.org/reading_room/whitepapers/awareness/ghosts-machine-who-why-attacks-information-security_914. Accessed 26 December 2013.

Becker, G. S. 1968. "Crime and Punishment: An Economic Approach," *Journal of Political Economy*, (76:2), pp.169–217.

Bentham, J. 1962. *Principles of penal law*, In *J. Bowring (Ed.)*, The works of Jeremy Bentham (pp. 396). New York: Russell and Russell.

Björkman, I., Fey, C. F., and Park, H. J. 2007. "Institutional Theory and MNC Subsidiary HRM Practices: Evidence from a Three Country Study," *Journal of International Business Studies*, (38:3), pp. 430–446.

Blumstein, A.1978. "*Introduction, in Deterrence and Incapacitation: Estimating the Effects of Criminal Sanctions on Crime Rates*," In *A. Blumstein, J. Cohen, and D. Nagin (Eds.)*, National academy of sciences. Washington, DC.

Boisot, M., and Child, J. 1996. "From Fiefs to Clans and Network Capitalism: Explaining China's Emerging Economic Order," Administrative *Science Quarterly*, 41, pp. 600-628.

Brooks, W.J., Warren, M.J., and Hutchinson, W. 2002. "A Security Evaluation Criteria," *Logistics Information Management*, (15:5/6), pp. 377-384.

Brouthers, K. D. 2002. "Institutional, Cultural and Transaction Cost Influences on Entry Mode Choice and Performance," *Journal of International Business Studies*, (33:2), pp. 203–222.

Carlsmith, K. M., Darley, J. M., and Robinson, P. H. 2002. "Why do We Punish?: Deterrence and Just Deserts as Motives for Punishment," *Journal of Personality and Social Psychology*, (83:2), pp. 284-299.

Carothers, T. 1998. "The Rule Law Revival," *Foreign Affairs*, (77:2), pp. 95-106.

Cate, F. 2008. Information Security Breaches. Faculty Publications, http://www.repository.law.indiana.edu/facpub/233. Accessed 20 December 2013.

Chaula, J. A. 2006. A Socio-technical Analysis of Information Systems Security Assurance: A Case Study for Effective Assurance. *Unpublished PhD Dissertation, Stockholm University, Sweden*.

Cline, J. 2006. Why isn't Europe Suffering a Wave of Security Breaches? http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9001176&pageNumber=2. Accessed 28 December 2013.

Computer Security Institute, 2011. CSI computer crime and security survey 2010/2011. http://gocsi.com/survey. Accessed 22 December 2013.

Cuervo-Cazurra, A., and Genc, M. 2008. "Transforming Disadvantages into Advantages: Developing-Country MNEs in the Least Developed Countries," *Journal of International Business Studies*, (39:6), pp. 957-979.

Delios, A., and Henisz, W. 2003. "Political Hazards, Experience, and Sequential Entry Strategies: The International Expansion of Japanese Firms, 1980–1998," *Strategic Management Journal*, (24:11), pp. 1153–1164.

Dhillon, G., and Torkzadeh, G. 2006. "Value-focused Assessment of Information Systems Security in Organizations," *Information Systems Journal*, (16:3), pp. 293-314.

DiMaggio, P. J., and Powell, W. W. 1983. "The Iron Cage Revisited: Institutional Isomorphism and Collective Rationality in Organizational Fields," *American Sociological Review*, 48, pp. 147-160.

Djankov, S., La Porta, R., Lopez-de-Silanes, F., and Shleifer, A. 2003. "Courts," *The Quarterly Journal of Economics*, (118:2), pp. 453-517.

Doh, J. P., and Pearce, J. A. 2004. "Corporate Entrepreneurship and Real Options in Transitional Policy Environments: Theory Development," *Journal of Management Studies*, 41, pp. 645-664.

Dols, T. and Silvius, G. 2010. "Exploring the Influence of National Cultures on Non-compliance Behaviors," *Communications of the IIMA*, (10:3), pp. 11.

Ellison, R., and Moore, A. 2003. Trustworthy Refinement through Intrusion-aware Design (TRIAD). http://web.archive.org/web/20070626170636/http://www.sei.cmu.edu/pub/documents/03.reports/pdf/03tr002.pdf. Accessed 18 December 2013.

Endicott, T. A. O. 1999. "The Impossibility of the Rule of Law," *Oxford Journal of Legal Studies*, (19:1), pp. 1-18.

Forcht, K. A. 1994. *Computer Security Management*. Boyd and Fraser: Danvers, MA.

Globerman, S., and Shapiro, D. 2003. "Governance Infrastructure and US Foreign Direct Investment," *Journal of International Business Studies*, (34:1), pp. 19–39.

Goodin, R. E. 1996. "Institutionalizing the Public Interest: The Defense of Deadlock and Beyond," *American Political Science Review*, pp. 331-343.

Gupta, A., and Hammond, R. 2005. "Information Systems Security Issues and Decisions for Small Businesses: An Empirical Examination," *Information Management & Computer Security*, (13:4), pp. 297-310.

Holburn, G. L., and Zelner, B. A. 2010. "Political Capabilities, Policy Risk, and International Investment Strategy: Evidence from the Global Electric Power Generation Industry," *Strategic Management Journal*, (31:12), pp. 1290-1315.

Hovav, A.,and D'Arcy, J. 2012. "Applying an Extended Model of Deterrence across Cultures: An Investigation of Information Systems Misuse in the U.S. and South Korea," *Information and Management*, 49, pp. 99-110.

Information Commissioner's Office. 2008. Guidance on Data Security Breach Management. http://www.ico.gov.uk/for_organisations/guidance_index/~/media/documents/library/Data_Protection/Practical_application/guidance_on_data_security_breach_management.ashx. Accessed 29 December 2013.

Jappelli, T., Pagano, M., and Bianco, M. 2005. "Courts and Banks: Effects of Judicial Enforcement on Credit Markets," *Journal of Money, Credit and Banking*, (37:2), pp. 223-244.

Kankanhalli, A., Teo, H. H., Tan, B. C., and Wei, K. K. 2003. "An Integrative Study of Information Systems Security Effectiveness," *International Journal of Information Management*, (23:2), pp. 139-154.

Kaufmann, D., Kraay, A., and Mastruzzi, M. 2009. "Governance Matters VIII: Aggregate and Individual Governance Indicators, 1996-2008," *World Bank Policy Research Working Paper*, 4978.

Knapp, K. J., Marshall, T. E., Rainer, R. K., and Ford, F. N. 2006. "Information Security: Management's Effect on Culture and Policy," *Information Management and Computer Security*, (14:1), pp. 24-36.

La Porta, R., López de Silanes, F., Shleifer, A., and Vishny, R. 1998. "Law and Finance," *Journal of Political Economy*, 106, pp. 1113-1155.

Li, S., and Filer, L. 2007. "The Effects of the Governance Environment on the Choice of Investment Mode and Strategic Implications," Journal *of World Business*, 42, pp.80-98.

Licht, A. N., Goldschmidt, C., and Schwartz, S. H. 2007. "Culture Rules: The Foundations of the Rule of Law and Other Norms of Governance," *Journal of Comparative Economics*, (35:4), pp. 659-688.

Luo, Y. 2007. "Are Joint Venture Partners more Opportunistic in a more Volatile Environment?" *Strategic Management Journal*, (28:1), pp. 39–60.

McAfee. 2005. *The Threats within*. McAfee.

Merryman, J. H. 1969. *The Civil Law Tradition: An Introduction to the Legal Systems of Western Europe and Latin American*. Stanford University Press.

Mishra, S. 2011. "Information Security Effectiveness: A Research Framework," *Issues in Information Systems*, (12:1), pp. 246-255.

North, D. C. 1990. *Institutions, Institutional Change, and Economic Performance*. Cambridge, MA: Harvard University Press.

Park, S. H., and Luo, Y. 2001. "Guanxi and Organizational Dynamics: Organizational Networking in Chinese Firms," *Strategic Management Journal*, 22, pp. 455-477.

Pelaez, M. 2010. *Measuring Effectiveness in Information Security Controls*. The SANS institute.

Peng, M. W. and Heath, P. S. 1996. "The Growth of the Firm in Planned Economies in Transition: Institutions, Organizations, and Strategic Choice," Academy *of Management Review*, 21, pp. 492-528.

Peng, M. W., and Khoury, T. A. 2008. "Unbundling the Institution-based View of International Business Strategy," *Oxford Handbook of International Business*, pp. 256-268.

Peng, M. W., and Zhou, J. Q. 2005. "How Network Strategies and Institutional Transitions Evolve in Asia," *Asia Pacific Journal of Management*, 22, pp. 321-336.

Phillips, L. and Votey, H. l. 1972. "An Economic Analysis of the Deterrent Effect of Law Enforcement on Criminal Activity," *The Journal of Criminal Law, Criminology, and Police Science*, (63:3), pp. 330-342.

Power, R. 2003. 2002 CSI/FBI Computer Crime and Security Survey. *Computer Security Issues and* Trends, 8(1), 1-21.

Reuters. 2011. Sony PlayStation Suffers Massive Data Breach. http://www.reuters.com/article/2011/04/26/us-sony-stoldendata-idUSTRE73P6WB20110426. Accessed 12 December 2013.

Richardson, R. 2009. CSI Computer Crime and Security Survey. Computer Security Institute, http://www.personal.utulsa.edu/~james-childress/cs5493/CSISurvey/CSISurvey2009.pdf. Accessed 15 December 2013.

Rosenzweig, P. M., and Singh, J. V. 1991. "Organizational Environments and the Multinational Enterprise," *Academy of Management Review*, (16:2), pp. 340-361.

Roy, J., and Oliver, C. 2009. "International Joint Venture Partner Selection: The Role of the Host-country Legal Environment," *Journal of International Business Studies*, 40, pp. 779-801.

Scholz, J. T. 1984. "Cooperation, Deterrence, and the Ecology of Regulatory Enforcement," *Law Society Review*, (18:2), pp. 179–224.

Scott, W. R. 2001. *Institutions and Organizations*. Thousand Oaks, CA: Sage.

Straub, D. 1990. "Effective IS Security: An Empirical Study," *Information Systems Research*, (1:3), pp. 255-276.

Straub, D. W., and Welke, R. J. 1998. "Coping with Systems Risk: Security Planning Models for Management Decision Making," *MIS Quarterly*, 22, pp. 441-470.

Symantec. 2012. Internet Security Threat Report. http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v18_2012_21291018.en-us.pdf. Accessed 12 December 2013.

VanCura, L. 2005. Building a Security Policy Framework for a Large, Multi-national Company. http://www.sans.org/reading_room/whitepapers/awareness/building-security-policy-framework-large-multi-national-company_1564. Accessed 20 December 2013.

Van Essen, M., Heugens, P. P., Otten, J., and Van Oosterhout, J. H. 2012. "An Institution-based View of Executive Compensation: A Multilevel Meta-analytic Test," *Journal of International Business Studies*, (43:4), pp. 396-423.

Visser, S., Hardin, B., Drage, J., Pinne, B., and Drage, J. 2012. Information Security & Data Breach Report. http://www.navigant.com/insights/library/disputes_and_investigations/2012/november_2012_update/. Accessed 11 December 2013.

Westney, D. E. 1993. "Institutionalization Theory and the Multinational Corporation," *Organization Theory and the Multinational Corporation*, 53, pp. 76.

Williams, K. R., and Hawkins, R. 1986. "Perceptual Research on General Deterrence: A Critical Review," *Law and Society Review*, pp. 545-572.

Yayla, A. 2011. "Enforcing Information Security Policies through Cultural Boundaries: A Multinational Company Approach," in *Proceedings of 2011 ECIS*, Paper 243, pp. 1-11.