Scientific Research Publishing

Beijing Law Review, 2020, 11, 637-650
https://www.scirp.org/journal/blr
ISSN Online: 2159-4635
ISSN Print: 2159-4627

An Institutional Theory Perspective on Developing a Cyber Security Legal Framework: A Case of Saudi Arabia

H. P. Singh[1]*, Tareq S. Alshammari[2]

[1]Department of MIS, College of Business Administration, University of Ha'il, Ha'il, KSA
[2]Department of Law, College of Shariah and Law, University of Ha'il, Ha'il, KSA
Email: *h.singh@uoh.edu.sa

How to cite this paper: Singh, H. P., & Alshammari, T. S. (2020). An Institutional Theory Perspective on Developing a Cyber Security Legal Framework: A Case of Saudi Arabia. *Beijing Law Review, 11,* 637-650.
https://doi.org/10.4236/blr.2020.113039

Received: May 13, 2020
Accepted: July 6, 2020
Published: July 9, 2020

Abstract

In the information age, the cyber-attacks have increased manifold, and developing a cyber-security legal framework is the need of the hour. Saudi Arabia experiences the highest cyber-attacks in the Arab region. This research attempts to develop a cyber-security legal framework for Saudi Arabia in particular and other countries in general. The study uses coercive, normative, and mimetic forces of institutional theory for this endeavor. Coercive pressure manifests in legal instruments, so countries like Saudi Arabia need to ensure compliance of their organizations to their respective laws, regulations, security policies, and procedures. Normative force manifests in professional networks and community expectations. So, countries like Saudi Arabia should collaborate, share information with other countries and join the Budapest Convention to combat cyber-crimes. Saudi Arabia should sufficiently incorporate the provisions of the Arab Convention on Combating Information Technology Offences in its legal instruments. Mimetic force involves copying the actions and practices of successful organizations. So, countries like Saudi Arabia should improve their legal tools by incorporating key features of legal instruments of more advanced cyber-secure nations like the UK, USA, Singapore, etc. Specifically, Saudi Arabia should improve its legal tools in the areas of privacy, identity theft, cyber-bullying, etc.

Keywords

Cyber-Attacks, Cyber-Crimes, Cyber-Security, Institutional Theory, Anti-Cyber Crime Law

1. Introduction

In the modern era, the Internet has emerged as the most important invention to

date. The dependence of organizations to leverage the Internet for meeting the customers' needs has been increasing day-by-day (Hunton, 2011). The use of the Internet for a variety of purposes by customers is increasing as well. By the year 2000, the Internet attracted 413 million users, and this exponentially increased to 3.4 billion in 2016 (Roser et al., 2020). The number of networked devices would increase from 17.1 billion to 27.1 billion in 2021 (Cisco, 2017). The increasing users and usage of the Internet has also made it susceptible to cyber-crimes and brought cyber-security issues to the forefront (Singh, 2017). The cyber-security problems have presented a dark side of the Internet as a platform on which the cyber-criminals have been able to grow and proliferate (Selwyn, 2007). It is difficult to punish cyber-criminals due to the abstract nature of the Internet and the complications involved in getting to the root of the origin of cyber-crimes (Hunton, 2011). These cyber-security issues pose severe threats to sensitive and private information (Joode, 2011). Such cyber-security challenges not only pose risks to individuals or businesses but countries as well. Such cyber-security challenges can threaten any country's national security, sociological balance, and financial position.

Countries across the globe have been experiencing increasing incidents of cyber-crimes. According to Clement (2019), the world regions affected by malicious data breaches (ranked by the share of attacks) in 2018 were: Asia Pacific (35%); North America (30%); Europe, Middle East & Africa (27%); and Latin America and the Caribbean (8%). According to Mihindukulasuriya (2020), the countries that experienced the most cyber-attacks in 2019 were: USA, India, UK, Singapore, Ukraine, Saudi Arabia, Nigeria, Japan, South Korea, and Spain respectively. In the Arab region, Saudi Arabia experiences the highest number of cyber-attacks, followed by the UAE (Forbes Middle East, 2018). Over the last few years, Saudi Arabia has witnessed major cyber-attacks like Shamoon on August 15, 2012; Cyber of emotion on August 15, 2015; Shamoon 2.0 on November 17, 2016, November 29, 2016, and January 23, 2017; Stone Drill in 2017; Mamba Ransomware in July 2017; Triton in August 2017; and Advanced Persistent Threat on November 20, 2017, etc. (Alshammari & Singh, 2018; Alelyani & Harish Kumar, 2018). In the year 2015 alone, Saudi Arabia faced 60 million cyber-attacks (Al-Hussein, 2017). From August 2016 to August 2017, 60 percent of the Saudi institutions faced cyber-attacks (Arab News, 2017). Estimates suggest that cyber-attacks would cost the Saudi economy up to US $8 billion (Bell, 2018). Also, estimates suggest that cyber-attacks would cost the world economy approximately $5.2 trillion from 2019 to 2023 (Ghosh, 2019).

Incidents of cyber-attacks carry a tremendous economic as well as social cost for all countries across the globe. The Middle East region has been one of the major victims of cyber-attacks. Saudi Arabia is worst affected by cyber-attacks in the Middle East region. So, this study stresses the importance of developing the cyber-security legal framework for Saudi Arabia. The knowledge generated by this study would be useful for Saudi Arabia, in particular, and the Middle East and other countries across the world in general. Accordingly, this study proposes

the following research questions:

RQ1: Which theory can contribute to the development of the cyber-security legal framework for Saudi Arabia in particular and other countries in general?

RQ2: How Saudi Arabia can leverage the proposed cyber-security legal framework in particular and other countries in general?

Technological, as well as legal interventions, are desired to address the cyber-security challenges. However, generally, technological advancements move at a rapid pace, but legal framework lags (Singh, 2016). This research looks at the problem from a legal approach to develop the cyber-security legal framework. This research paper is divided into six sections to present the research approach. Section 2 is dedicated to the review of the literature. This research makes a case for applying institutional theory to develop a cyber-security legal framework for Saudi Arabia in particular and other countries in general. Accordingly, in sub-Section 2.1, the authors present the tenets of institutional theory. In Sections 3 and 4, the authors examine the tenets of institutional theory in the legal context of Saudi Arabia. In Section 3, the authors examine the Saudi cyber-security related laws, policies and procedures, membership of convention(s), the performance of Saudi Arabia in the legal pillar of GCI index vis-à-vis leading nations. In Section 4, the authors depict the application of three forces of institutional theory for developing a cyber-security legal framework for Saudi Arabia in particular and other countries in general. Section 5 presents the discussion based on the research work in Sections 1 to 4. Section 6 concludes the research paper.

2. Literature Review

The literature presents numerous ideas for the assessment of cyber-security at the organizational level. International Organization for Standardization/International Electro-technical Commission (ISO/IEC) standard 27000-4 and National Institute of Standards and Technology (NIST) security metric guide presents the definition and operationalization of security measurements (Chew et al., 2008). The CORAS approach presents a meta-model over the security field to support cyber-security assessments (Lund et al., 2011). Breu et al. (2008) extend the model-based approach to security management and identify the cyber-security threats that have the sturdiest influence on business security objectives. Hallberg et al. (2006) proposed the XMASS method by which modeler can specify cyber-security profiles for business entities and calculate cyber-security values. However, all the above cyber-security assessment methods apply to business organizations and not to countries. Further, they can provide cyber-security assessment and not a cyber-security legal framework.

At the country level, a study was conducted by Alshammari & Singh (2018) to assess the preparedness of Saudi Arabia to defend itself against cyber-crimes. The study made an assessment based on Saudi Anti-Cyber Crime Law (2007) and the Global Cyber-security Index (GCI) of 2017. The study found Saudi Arabia in the maturing stage of the GCI index of 2017 behind leading countries like Singapore, the USA, Malaysia, Oman, Mauritius, Australia, Russia, Egypt, etc.

Despite a comprehensive assessment, this study did not provide a cyber-security legal framework. Also, this study only focused on the Saudi Anti-Cyber Crime Law (2007) and did not consider other Saudi legislations like the Telecom Act (2001) and Electronic Transactions Law (2007).

Gandhi (2014) compares cyber-attacks to pathogen infections (e.g., COVID-19) and argues that cyber-systems are complex adaptive systems, so principles of complexity science (like system thinking and natural science) should be leveraged in the cyber-security field to complement traditional approaches. The paper presents high-level techniques in this endeavor. The article states that the holism approach to cyber-security is better than the reductionist approach having specific point solutions to individual problems. The author suggests the building of diversity in cyber-security systems to increase their immunity to cyber-attacks. The author also indicates that simulation modeling techniques like Agent-Based Modelling should be used to model cyber-security systems. However, the author merely presents several theoretical ideas but does not suggest the mechanisms of their implementation. Also, the author presents complexity science in the context of organizations and does not consider the country as an entity for the implementation of the theoretical framework proposed by him.

Björck (2004) states that the social behavior of humans' impacts cyber-security. So, they present arguments to deploy institutional theory in Information System/Information Technology (IS/IT) security research. The authors give various examples of the use of institutional theory in IS/IT research and make a case in favor of using institutional theory in IS/IT security. They state that the institutional perspective can help to achieve a sound and cost-effective IS/IT security management infrastructure. Hovav & D'Arcy (2012) call for applying institutional theory to understand better compliance of organizations with information security regulations, standards, and policies.

According to Teo et al. (2003), the institutional theory provides insights into the significance of institutional environments to organizational structures and actions. According to Currie (2009), the institutional theory provides rich observations regarding non-linear routes of IT adoption across organizations.

The authors have found the applications of institutional theory in various researches related to IS/IT at individual and organizational levels. Institutional theory has been applied for financial electronic data interchange (FEDI) adoption at the organizational level by Teo et al. (2003). Butler (2003) used institutional theory to describe, explain, and understand the role of social forces in the development of web-based information systems in organizations. Cavalluzzo & Ittner (2004) establish that leveraging legislative instruments impacts the adoption of management control systems and increases operational productivity in public organizations. Liang et al. (2007) leveraged institutional theory and demonstrated the substantial impact of existing rules and regulations, and public opinions in the assimilation of enterprise systems. Ugrin (2009) has applied institutional theory for enterprise resource planning (ERP) adoption at the orga-

nizational level. Shi et al. (2008) have applied institutional theory for internet banking adoption at the individual level. Sherer (2010) has applied institutional theory for physicians' adoption of Electronic Health Records (EHRs). Burnett et al. (2015) have applied institutional theory to analyze hospital responses to external demands for finance and quality in 5 European countries.

Despite multiple applications of institutional theory in the IS/IT field in general and the recommendations of Björck (2004) and Hovav & D'Arcy (2012) to apply it in IS/IT security, there are scant attempts to apply it in the critical area of cyber-security. The authors select this theory due to its scope and its lack of application to the area of cyber-security. Also, the authors would apply it at the level of the country, instead of an organizational or individual level.

Institutional Theory

Institutional theory has its roots in social science disciplines like ethnography, political science, anthropology, phenomenology, and organization studies. This study applies the institutional model of isomorphic change by DiMaggio & Powell (1983). The model of DiMaggio & Powell (1983) is widely used to understand the influence of institutional forces on the information security compliance of organizations. This model stresses the importance of conforming to external expectations to secure legitimacy from stakeholders for organizations (Appari et al., 2009). Cavusoglu et al. (2015) state that this legitimacy can be secured by strategically responding to external pressures.

According to DiMaggio & Powell (1983), organizations converge to similar practices and behaviors over a while. They identified and explained three forces that determine how adopted behaviors and practices become isomorphic-ally accepted by the organization field as a whole. These three forces are: coercive (constraining), normative (learning), and mimetic (cloning) (Davidsson et al., 2006; Cavusoglu et al., 2015). Political influence and organizational legitimacy derive coercive isomorphism. It can be conveyed through laws, regulations, policies, outside agency standardization, oversight, or compliance requirements (Cavusoglu et al., 2015; Kim et al., 2016). Normative isomorphism is related to professional values and norms embedded in the organization (Appari et al., 2009). It can stem from learning from others in professional networks. It can also stem from the expectations of the community from organizations to act in a certain manner at a specific time (Appari et al., 2009; Kam & Katerattanakul, 2014). Mimetic isomorphism involves copying or mimicking the behaviors of others. These behaviors are a result of organizational response to uncertainty, and cause them to imitate success actions and practices of similar organizations within their environment (Safa et al., 2016). The publicity of perceived benefits by organizations creates pressure on other organizations to adopt similar actions and practices (Alkalbani et al., 2017). According to DiMaggio & Powell (1983), by examining and measuring the organizational field around these three forces, it is possible to understand convergence on homogenized practices and accepted behaviors in organizations. So coercive, normative, and mimetic pressures guide

the institutionalization of organizations.

Based on the above tenets, the three forces (coercive, normative, and mimetic) of institutional theory can contribute to the development of the cyber-security legal framework for Saudi Arabia in particular and other countries in general.

3. Cyber Security Legal Position of Saudi Arabia

In Saudi Arabia, some laws contain provisions related to cyber-security like Telecom Act (2001), Anti-Cyber Crime Law (2007), and Electronic Transactions Law (2007).

The Telecom Act (2001) established the Saudi Communications Commission (SCC). The act provides supervisory guidelines and regulations for the telecom sector. It empowers the SCC to set the national numbering plan, access rights, grant licenses, and state the rules of competition. It protects the privacy and confidentiality of people. Also, it states violations and penalties under article 37.

The Anti-Cyber Crime Law (2007) defines un-authorized access as deliberate, unauthorized access by any person to computers, websites, information systems, and computer networks. It identifies various cyber-crimes and determines their punishments. It contains penal provisions against prevention of data interception (Article 3(1)), data interference ((Articles 3(3)) and 5(2)), system interference (Article 7(2)), illegal access (Articles 3(2), 4(2) and 5(1)), invasion of privacy (Article 3(4)), cyber-terrorism (Article 7(1)), and attempts to commit cyber-crime (Article 10). It also contains provisions regarding the maintenance of public order and morals (Articles 6(1), 6(2), 6(3), and 6(4)). The punishment for various cyber-crime offenses can range from imprisonment for a period from one to ten years and/or a fine from a few thousand to five million Saudi Riyals. It also stipulates the Communications and Information Technology Commission along with competent security agencies and Bureau of Investigation and Public Prosecution as investigation and persecution bodies (Articles 14 and 15).

The Electronic Transactions Law (2007) defines electronic transactions, electronic records, electronic signature, digital certificate, certification service provider, etc. (Article 1). It aims to control, regulate, and provide a legal framework for electronic transactions and signatures (Article 2). The act provides legal validity to electronic transactions, records, and signatures (Article 5). This law provides for offer and acceptance of contracts in electronic form (Article 10). It confers electronic signature as equal status to the handwritten signature (Article 14). The act defines the powers of the Ministry of Communications and Information Technology, and Communication and Information Technology Commission (Article 15). It makes provision for establishing a national center for digital certification (Article 16), and obligations and responsibilities of certification service providers (Article 17). It defines the duties of the certificate holder (Article 22). It contains provisions of penalties for various electronic offenses like providing false or misleading information, forging electronic records, signatures or digital certificates, identity theft, etc. (Article 23).

Saudi Arabia has also developed the Information Security Policies and Procedures Development Framework for Government Agencies (CITC, 2011). It contains information security policies and guidelines that assist Saudi government agencies in managing their information security risks. Saudi Arabia also formed the Parental Control Service Regulatory Framework (CITC, 2017) to protect children from internet risks and prevent abuse on social media, etc.

Cyber-attacks occur beyond the country boundaries through a network of intermediary systems that mask the attackers' identity (Grabosky, 2014). So, countries need to collaborate and share information. Saudi Arabia is a member of the Arab League. It shares cultural, political, and socio-economic interests with Arab League countries (Alazab & Chon, 2015). Arab countries formed a platform to enhance cooperation among themselves to combat cyber-crimes—the Arab Convention on Combating Information Technology Offences (ACCITO, 2015). The convention covers cyber-crimes involving more than one state (Article 3). The convention covers offenses of illicit access (Article 6), illicit interpretation (Article 7), compromising the integrity of data (Article 8), misuse of Information Technology means (Article 9), online forgery (Article 10), cyber fraud (Article 11), cyber pornography (Articles 12 and 13), cyber-piracy (Article 14), cyber-terrorism (Article 15), organized cyber-crimes (Article 16), violation of copyright (Article 17), illicit use of electronic payment tools (Article 18), the attempt at and participation in the commission of offenses (Article 19), etc. The convention calls on member states to increase punishment for cyber-crimes (Article 21) and to mutually assist each other for investigating and combating crimes (Article 32). Despite signatory, Saudi laws related to cyber-security do not mention or sufficiently incorporate the provisions of this convention. Saudi Arabia and other countries of the Gulf Cooperation Council (GCC) have not joined the Budapest convention, which is a comprehensive international treaty for cyber-crime investigation and law (Council of Europe, 2020).

Saudi Arabia had improved its position in the GCI index of 2018 to 13th rank from 46th rank in 2017. As per the GCI index of 2018, the leading cyber-secure countries are the UK, USA, and Singapore, etc. UK has strong legal instruments to fight cyber-crimes like Computer Misuse Act 1990, Communications Act 2003, General Data Protection Regulation, Network and Information Security Regulations 2018, Privacy and Electronic Communications (EC Directive) Regulations 2003, etc. (Timmons et al., 2019). USA possesses strong legal instruments to combat cyber-crimes like the Computer Fraud and Abuse Act (CFAA) of 1986, the US National Information Infrastructure Protection Act (NIIA) of 1996, Wiretap Act, and Network Crime Statutes, etc. (Floyd, 2016). Singapore possesses comprehensive cyber-security legal instruments like Cybersecurity Act 2018, Computer Misuse Act, Personal Data Protection Act 2012, Cybersecurity (Critical Information Infrastructure) Regulations 2018, Cybersecurity (Confidential Treatment of Information) Regulations 2018, etc. (Ting & Kin, 2019). Saudi Arabia still lags behind leading nations in the legal pillar as per GCI Index of 2018 and needs improvement.

4. Institutional Theory for Developing Cyber-Security Legal Framework

In this section, the authors present the application of institutional theory for developing the cyber-security legal framework for Saudi Arabia in particular and other countries in general. In the case of countries like Saudi Arabia, the three forces (coercive, normative, and mimetic) under institutional theory are applicable. Table 1 depicts this.

5. Discussion

Countries across the globe have been witnessing increasing incidents of cyber-crimes. In the Arab region, Saudi Arabia has been the worst hit by cyber-crimes. To successfully defend against cyber-crimes, countries like Saudi Arabia need a cyber-security legal framework.

The literature presents various cyber-security assessment methods like ISO/IEC standard 27000-4, NIST security metric guide, CORAS approach, XMASS method, etc. However, these methods apply to business organizations,

Table 1. Institutional theory for developing cyber-security legal framework.

Force	Developing a Cyber Security Legal Framework
Coercive	Coercive force in cyber-security is visible in Saudi Arabia in the form of legal instruments like Telecom Act (2001), Anti-Cyber Crime Law (2007), Electronic Transactions Law (2007), Information Security Policies and Procedures Development Framework for Government Agencies (CITC, 2011), Parental Control Service Regulatory Framework (CITC, 2017), etc. The presence of such laws, policies, and procedures create legal pressure on organizations to act in compliance to gain acceptability from the government (Edwards et al., 2009). Such legislative requirements increase information security compliance in organizations (Smith & Jamieson, 2006). Countries such as Saudi Arabia need to ensure that various institutions comply with these coercive legal instruments.
Normative	In developing countries like Saudi Arabia, community pressures influence information security compliance in public organizations (Kam & Katerattanakul, 2014). Privacy, trust, and quality of services are socially desirable needs, and organizations need to address them to maintain their reputation in the information era (Zhang et al., 2005). To enhance cooperation with Arab League countries, Saudi Arabia needs to incorporate provisions of the Arab Convention on Combating Information Technology Offences in its legal instruments. Countries like Saudi Arabia should standardize their laws in line with international conventions (Singh, 2018a). They should also join the Budapest convention to build cooperative and collaborative relationships with the international community.
Mimetic	In countries like Saudi Arabia, who still need to make progress in the area of cyber-security, mimicking the cyber-security practices, more advanced nations like the UK, the USA, and Singapore, etc. can be done. Such mimicking can help to minimize risks and threats, increase stakeholders' confidence and trust, and improve people's confidence due to enhanced security (Singh & Agarwal, 2011; Singh & Grover, 2011; Steinbart et al., 2012; Singh, 2018b). Saudi Arabia has Anti-Cyber Crime Law (2007), but it is deficient in preventing protecting the privacy of individuals, theft of identity, preventing cyber-bullying, etc. (Alshammari & Singh, 2018). Saudi Arabia needs to make these improvements in its legal framework mimicking the actions and practices of more advanced countries as per the GCI Index of 2018.

not countries. Alshammari & Singh (2018) assessed the preparedness of Saudi Arabia vis-à-vis Anti-Cyber Crimes Law and GCI index of 2017 but did not provide a cyber-security legal framework. Gandhi (2014) presents theoretical ideas to model cyber-security systems but does not present implementation mechanisms.

The institutional theory has been applied to multiple IS/IT studies. At the organizational level, institutional theory has been applied in IS/IT by Teo et al. (2003), Butler (2003), Cavalluzzo & Ittner (2004), Liang et al. (2007), Ugrin (2009), Burnett et al. (2015), etc. At the individual level, institutional theory has been applied in IS/IT by Sherer (2010), Shi et al. (2008), etc. There is hardly any study in the area of cyber-security, where institutional theory has been applied. Authors like Björck (2004) and Hovav & D'Arcy (2012) recommended the application of institutional theory in IS/IT security. Due to its scope, institutional theory has been selected and applied in this research to develop a cyber-security legal framework. This answers the first research question (RQ1).

To answer the second research question (RQ2), the authors examined the tenets of institutional theory as well as Saudi cyber-security related laws, policies and procedures, membership of convention(s), the performance of Saudi Arabia in GCI index vis-à-vis leading countries. According to Institutional theory, three forces guide the behavior of organizations: coercive, normative, and mimetic (Davidsson et al., 2006; Cavusoglu et al., 2015). Coercive force is visible in the form of legal instruments (Cavusoglu et al., 2015; Kim et al., 2016). In Saudi Arabia, the coercive legal tools are Telecom Act (2001), Anti-Cyber Crime Law (2007), Electronic Transactions Law (2007), Information Security Policies and Procedures Development Framework for Government Agencies (CITC, 2011), Parental Control Service Regulatory Framework (CITC, 2017), etc. Normative force is visible in the form of professional networks and community expectations (Appari et al., 2009; Kam & Katerattanakul, 2014). Saudi Arabia is a member of the Arab Convention on Combating Information Technology Offences (ACCITO, 2015). Mimetic force involves copying or mimicking the actions and practices of successful organizations (Safa et al., 2016). Saudi Arabia is behind countries like the UK, the USA, and Singapore, etc. in the legal pillar of the GCI Index of 2018 and needs to mimic them to sharpen its cyber-security legal framework. By complying with the three forces of institutional theory, countries like Saudi Arabia can leverage the cyber-security legal framework. This answers the second research question (RQ2).

6. Conclusion

In the modern era, increasing users of internet and networking devices have brought cyber-security challenges to the forefront. To address these challenges and keep cyber-criminals at bay, countries like Saudi Arabia need to develop their cyber-security legal framework. The three forces of institutional theory (coercive, normative, and mimetic) present a proper structure to develop such a cyber-security legal framework. Although Saudi Arabia possesses coercive legal

cyber-security tools, however, countries like Saudi Arabia need to ensure the compliance of organizations to these legal instruments. In partial compliance of normative force, Saudi Arabia is a member of the Arab Convention on Combating Information Technology Offences. However, countries like Saudi Arabia need to sufficiently incorporate provisions of this convention in its cyber-security legal instruments. Also, Saudi Arabia and other Arab League countries should join the Budapest Convention and should standardize their laws in line with this international convention. They should collaborate and share information with other countries. Although Saudi Arabia has improved its position in the GCI Index of 2018 as compared to 2017, it is still behind the leading nations in the legal pillar of the GCI index. So, countries like Saudi Arabia need to strengthen their legal instruments by learning from more cyber-secure nations like the UK, USA, and Singapore, etc. Specifically, Saudi Arabia needs to improve its Anti-Cyber Crime Law (2007) in the areas of privacy, identity theft, cyber-bullying, etc.

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

ACCITO (9 March 2015). *Arab Convention on Combating Information Technology Offences*. https://www.asianlaws.org/gcld/cyberlawdb/GCC/Arab%20Convention%20on%20Combating%20Information%20Technology%20Offences.pdf

Alazab, M., & Chon, S. (2015). Cyber Security in the Gulf Cooperation Council. *SSRN Electronic Journal,* 1-3. https://doi.org/10.2139/ssrn.2594624

Alelyani, S., & Harish Kumar, G. R. (2018). Overview of Cyberattack on Saudi Organizations. *Journal of Information Security and Cybercrimes Research, 1,* 42-50. https://doi.org/10.26735/16587790.2018.004

Al-Hussein, I. (2 May 2017). *60 Million Cyber-Attacks Targeted Saudi Arabia in One Year*. https://english.alarabiya.net/en/media/digital/2017/05/02/60-million-cyber-attacks-targeted-Saudi-Arabia-in-one-year

Alkalbani, A., Deng, H., Kam, B., & Zhang, X. (2017). Information Security Compliance in Organizations: An Institutional Perspective. *Data and Information Management, 1,* 104-114. https://doi.org/10.1515/dim-2017-0006

Alshammari, T. S., & Singh, H. P. (2018). Preparedness of Saudi Arabia to Defend Against Cyber Crimes: An Assessment with Reference to Anti-Cyber Crime Law and GCI Index. *Archives of Business Research, 6,* 131-146. https://doi.org/10.14738/abr.612.5771

Anti-Cyber Crime Law (2007). *Communications and Information Technology Commission*. https://www.citc.gov.sa/en/RulesandSystems/CITCSystem/Pages/CybercrimesAct.aspx

Appari, A., Johnson, M. E., & Anthony, D. L. (2009). HIPAA Compliance: An Institutional Theory Perspective. *Proceedings of the 15th Americas Conference on Informa-*

tion Systems, San Francisco, CA 6-9 August 2009, 252-261.

Arab News (29 September 2017). *Study: 60% of Saudi Institutions Hit by Virus Attacks, Malware*. https://www.arabnews.com/node/1169846/saudi-arabia

Bell, J. (21 July 2018). *KSA Must Become More Resilient against Cyberattacks.* https://www.arabnews.com/node/1343151/saudi-arabia

Björck, F. (2004). Institutional Theory: A New Perspective for Research into IS/IT Security in Organisations. *Proceedings of the 37th Annual Hawaii International Conference on System Sciences*, Big Island, HI, 5-8 January 2004, 1-5. https://doi.org/10.1109/HICSS.2004.1265444

Breu, R., Innerhofer-Oberperfler, F., & Yautsiukhin, A. (2008). Quantitative Assessment of Enterprise Security System. *2008 3rd International Conference on Availability, Reliability and Security*, Barcelona, 4-7 March 2008, 921-928. https://doi.org/10.1109/ARES.2008.164

Burnett, S., Mendel, P., Nunes, F., Wiig, S., Bovenkamp, H. V., Karltun, A., Robert, G., Anderson, J., Vincent, C., & Fulop, N. (2015). Using Institutional Theory to Analyze Hospital Responses to External Demands for Finance and Quality in Five European Countries. *Journal of Health Services Research & Policy, 21,* 109-117. https://doi.org/10.1177/1355819615622655

Butler, T. (2003). An Institutional Perspective on Developing and Implementing Intranet- and Internet-Based Information Systems. *Information Systems Journal, 13,* 209-231. https://doi.org/10.1046/j.1365-2575.2003.00151.x

Cavalluzzo, K. S., & Ittner, C. D. (2004). Implementing Performance Measurement Innovations: Evidence from Government. *Accounting, Organizations and Society, 29,* 243-267. https://doi.org/10.1016/S0361-3682(03)00013-8

Cavusoglu, H., Cavusoglu, H., Son, J.-Y., & Benbasat, I. (2015). Institutional Pressures in Security Management: Direct and Indirect Influences on Organizational Investment in Information Security Control Resources. *Information & Management, 52,* 385-400. https://doi.org/10.1016/j.im.2014.12.004

Chew, E., Swanson, M., Stine, K. M., Bartol, N., Brown, A., & Robinson, W. (2008). Performance Measurement Guide for Information Security. *NIST Special Publication 800-55 Revision 1,* 1-40. https://doi.org/10.6028/NIST.SP.800-55r1

Cisco (7 June 2017). *The Zettabyte Era: Trends and Analysis*. https://www.cisco.com/c/en/us/solutions/

CITC (17 September 2017). *Parental Control Service Regulatory Framework*. https://www.citc.gov.sa/en/new/publicConsultation/Pages/143804.aspx

CITC (2011). *Information Security Policies and Procedures Development Framework for Government Agencies*. https://www.citc.gov.sa/en/RulesandSystems/RegulatoryDocuments/OtherRegulatoryDocuments/Documents/CITC_Information_Security_Policies_and_Procedures_Guide_En.pdf

Clement, J. (22 July 2019). *Cyber-Crime: Most-Targeted Victim Countries 2018*. https://www.statista.com/statistics/256653/most-targeted-victim-countries-of-cyber-attacks/

Council of Europe (2020). *Parties/Observers to the Budapest Convention and Observer Organisations to the T-CY*. https://www.coe.int/en/web/cybercrime/parties-observers

Currie, W. (2009). Contextualizing the IT Artefact: Towards a Wider Research Agenda for IS Using Institutional Theory. *Information Technology & People, 22,* 63-77. https://doi.org/10.1108/09593840910937508

Davidsson, P., Hunter, E., & Klofsten, M. (2006). Institutional Forces: The Invisible Hand that Shapes Venture Ideas? *International Small Business Journal: Researching Entrepreneurship, 24,* 115-131. https://doi.org/10.1177/0266242606061834

DiMaggio, P. J., & Powell, W. W. (1983). The Iron Cage Revisited: Institutional Isomorphism and Collective Rationality in Organizational Fields. *American Sociological Review, 48,* 147-160. https://doi.org/10.2307/2095101

Edwards, J. R., Mason, D. S., & Washington, M. (2009). Institutional Pressures, Government Funding and Provincial Sport Organizations. *International Journal of Sport Management and Marketing, 6,* 128-149. https://doi.org/10.1504/IJSMM.2009.028798

Electronic Transactions Law (2007). *Communications and Information Technology Commission*. https://www.citc.gov.sa/en/RulesandSystems/CITCSystem/Pages/ElectronicTransactionsLaw.aspx

Floyd, J. T. (8 March 2016). *A Guide to Cyber Crime Laws*. https://www.johntfloyd.com/

Forbes Middle East (28 March 2018). *Arab Countries Facing the Highest Number of Cyber Attacks*. https://www.forbesmiddleeast.com/en/

Gandhi, G. (May 2014). *Complexity Theory in Cyber Security*. http://cognitsolutions.blogspot.com/p/complexity-in-cyber-security.html

Ghosh, I. (7 November 2019). *This Is the Crippling Cost of Cybercrime on Corporations*. https://www.weforum.org/agenda/2019/11/cost-cybercrime-cybersecurity/

Grabosky, P. (2014). The Evolution of Cybercrime, 2004-2014. *SSRN Electronic Journal,* RegNet Research Paper No. 2014/58. https://doi.org/10.2139/ssrn.2535605

Hallberg, J., Hallberg, N., & Hunstad, A. (2006). *Crossroads and XMASS: Framework and Method for System IT Security Assessment*. Linköping: Total Försvarets Forskningsinstitut (FOI).

Hovav, A., & D'Arcy, J. (2012). Applying an Extended Model of Deterrence Across Cultures: An Investigation of Information Systems Misuse in the US and South Korea. *Information & Management, 49,* 99-110. https://doi.org/10.1016/j.im.2011.12.005

Hunton, P. (2011). A Rigorous Approach to Formalising the Technical Investigation Stages of Cybercrime and Criminality within a UK Law Enforcement Environment. *Digital Investigation, 7,* 105-113. https://doi.org/10.1016/j.diin.2011.01.002

Joode, A. D. (2011). Effective Corporate Security and Cybercrime. *Network Security, 2011,* 16-18. https://doi.org/10.1016/S1353-4858(11)70097-6

Kam, H.-J., & Katerattanakul, P. (2014). Information Security in Higher Education: A Neo-Institutional Perspective. *Journal of Information Privacy and Security, 10,* 28-43. https://doi.org/10.1080/15536548.2014.912482

Kim, D.-J., Hwang, I.-H., & Kim, J.-S. (2016). A Study on Employees Compliance Behavior towards Information Security Policy: A Modified Triandis Model. *Journal of Digital Convergence, 14,* 209-220. https://doi.org/10.14400/JDC.2016.14.4.209

Liang, H., Saraf, N., Hu, Q., & Xue, Y. (2007). Assimilation of Enterprise Systems: The Effect of Institutional Pressures and the Mediating Role of Top Management. *MIS Quarterly, 31,* 59-87. https://doi.org/10.2307/25148781

Lund, M. S., Solhaug, B., & Stølen, K. (2011). *Model-Driven Risk Analysis—The CORAS Approach*. Berlin: Springer. https://doi.org/10.1007/978-3-642-12323-8

Mihindukulasuriya, R. (3 March 2020). *India Was the Most Cyber-Attacked Country in the World for Three Months in 2019*. https://theprint.in/tech/india-was-the-most-cyber-attacked-country-in-the-world-for-three-months-in-2019/374622/

Roser, M., Ritchie, H., & Ortiz-Ospina, E. (2020). *Internet*. https://ourworldindata.org/internet

Safa, N. S., Solms, R. V., & Furnell, S. (2016). Information Security Policy Compliance Model in Organizations. *Computers & Security, 56,* 70-82. https://doi.org/10.1016/j.cose.2015.10.006

Selwyn, N. (2007). A Safe Haven for Misbehaving? *Social Science Computer Review, 26,* 446-465. https://doi.org/10.1177/0894439307313515

Sherer, S. A. (2010). Information Systems and Healthcare XXXIII: An Institutional Theory Perspective on Physician Adoption of Electronic Health Records. *Communications of the Association for Information Systems, 26,* 127-140. https://doi.org/10.17705/1CAIS.02607

Shi, W., Shambare, N., & Wang, J. (2008). The Adoption of Internet Banking: An Institutional Theory Perspective. *Journal of Financial Services Marketing, 12,* 272-286. https://doi.org/10.1057/palgrave.fsm.4760081

Singh, H. P. (2016). E-Commerce Security: Legal and Policy Aspects of Technology Solutions in India. *Mumukshu Journal of Humanities, 8,* 13-19.

Singh, H. P. (2017). Strategic Analysis and Security Issues of Social Media Services: A Study of Facebook. *International Journal of Information Movement, 2,* 134-139.

Singh, H. P. (2018a). Domain Name Disputes and Their Resolution under UDRP Route: A Review. *Archives of Business Research, 6,* 147-156. https://doi.org/10.14738/abr.612.5786

Singh, H. P. (2018b). Data Protection and Privacy Legal-Policy Framework in India: A Comparative Study vis-à-vis China and Australia. *Amity Journal of Computational Sciences, 2,* 24-29.

Singh, H. P., & Agarwal, A. (2011). Espousal of E-Learning in Adult Education. In *Proceedings of the International Conference on Computational Techniques and Artificial Intelligence* (pp. 28-31). Pattaya, Thailand: ISEM-Planetary Scientific Research Centre. https://www.researchgate.net/publication/311104278_Espousal_of_E-Learning_in_Adult_Education

Singh, H. P., & Grover, S. T. (2011). Marketing of E-Banking Services: A Critical Analysis on Lifecycle Demographics, Enabling and Disabling Factors. *Zenith International Journal of Multidisciplinary Research, 1,* 20-38.

Smith, S., & Jamieson, R. (2006). Determining Key Factors in E-Government Information System Security. *Information Systems Management, 23,* 23-32. https://doi.org/10.1201/1078.10580530/45925.23.2.20060301/92671.4

Steinbart, P. J., Raschke, R. L., Gal, G., & Dilla, W. N. (2012). The Relationship between Internal Audit and Information Security: An Exploratory Investigation. *International Journal of Accounting Information Systems, 13,* 228-243. https://doi.org/10.1016/j.accinf.2012.06.007

Telecom Act (2001). *Communications and Information Technology Commission*. https://www.citc.gov.sa/en/RulesandSystems/CITCSystem/Pages/TelecommunicationsAct.aspx

Teo, H. H., Wei, K. K., & Benbasat, I. (2003). Predicting Intention to Adopt Inter-Organizational Linkages: An Institutional Perspective. *MIS Quarterly, 27,* 19-49. https://doi.org/10.2307/30036518

Timmons, J., Chabinsky, S. R., & Pittman, F. P. (1 May 2019). *Cybersecurity and the UK Legal Landscape*. https://www.whitecase.com/publications/alert/cybersecurity-and-uk-legal-landscape

Ting, S., & Kin, L. C. (25 February 2019). *Cybersecurity in Singapore.* https://www.lexology.com/library/detail.aspx?g=e8e0c6b8-d81a-4dfc-a8fe-36a1dd3baa54

Ugrin, J. C. (2009). The Effect of System Characteristics, Stage of Adoption, and Experience on Institutional Explanations for ERP Systems Choice. *Accounting Horizons, 23,* 365-389. https://doi.org/10.2308/acch.2009.23.4.365

Zhang, J., Dawes, S. S., & Sarkis, J. (2005). Exploring Stakeholders Expectations of the Benefits and Barriers of E-Government Knowledge Sharing. *Journal of Enterprise Information Management, 18,* 548-567. https://doi.org/10.1108/17410390510624007