International Journal of Information Technology and Management

Vol. VI, Issue No. I, February-2014, ISSN 2249-4510

ANALYTICAL STUDY ON THE EMERGENCE OF CYBER SECURITY LAW

AN INTERNATIONALLY INDEXED PEER REVIEWED & REFEREED JOURNAL

www.ignited.in

International Journal of Information Technology and Management
Vol. VI, Issue No. I, February-2014, ISSN 2249-4510

Analytical Study on the Emergence of Cyber Security Law

Pelasur Chandrakumar Swamy

Research Scholar, Himalayan University, Arunachal Pradesh

Abstract – This paper examines cyber law as a growing field of legal practice and the roles that lawyers play in helping companies respond to cyber security threats. Drawing on interviews with lawyers, consultants, and academics knowledgeable in the intersection of law and cyber security, as well as a survey of lawyers working in general counsel's offices, this study examines the broader context of cyber security, the current legal framework for data security and related issues, and the ways in which lawyers learn about and involve themselves in cyber security issues. Cyber law is a term that encapsulates the legal issues related to use of communicative, transactional, and distributive aspects of networked information devices and technologies. It is less a distinct field of law in the way that property or contract are, as it is a domain covering many areas of law and regulation.

Keywords: Cyber Law, Cyber Security, Lawyers, Communicative, Security, Growing, etc.

----------♦----------

INTRODUCTION

Over the past year, a number of high profile data security breaches at large retailers and broad-reaching security threats like the Heart bleed Bug, have heightened public awareness about the threat of cyber-attacks to personal information [1]. Moreover, according to a 2013 study on the cost of cybercrime by the Ponemon Institute, the United States led nine other nations in highest average organizational cost-per-breach and largest average number of breached records. According to the same survey, the annualized cost of cybercrime increased by 30 percent from 2012 to 2013, now estimated at $11.6 million per year per company studied. As a result, cyber security has emerged as a primary concern for many corporate leaders [2]. A 2014 survey of nearly 500 company directors and general counsel found that "data security" was the number one issue for directors that "keeps them up at night," and the second most important issue for general counsel, after regulatory compliance [3]. Similarly, among the corporate law departments surveyed for this study, a majority rated cyber security as a "high concern," both company-wide and within the law department [4].

REVIEW OF LITERATURE:

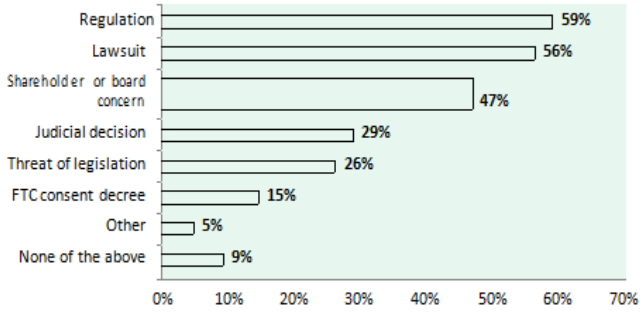
The broad range of negative impacts that a successful cyber threat poses to companies drive such concerns– financial loss is just one of the problems that can result from a breach. In 2012, for instance, PricewaterhouseCoopers found that about 38 percent of businesses experience financial losses as a result of cyber security incidents, but that similar numbers also suffer intellectual property theft and brand or reputation damage [5]. Indeed, given the often highly publicized nature of cyber security breaches, reputation damage may be one of the greatest threats this risk poses [6]. Among the corporate law departments surveyed for this study, the cyber security consequence respondents ranked as their top concern is "Potential for damage to reputation with customers"; purely legal consequences, such as regulatory action or lawsuits, were ranked lower, with loss of shareholder confidence ranking lowest. Almost half of respondents gave a rank of 1 or 2 to "Potential for damage to reputation with customers" or "Loss of company's intellectual property," while only about a quarter gave such ratings to "Potential for loss of confidence among shareholders/investors [7]."

1- Corporate Cyber security Preparedness:

Cyber security clearly has the attention of corporate leaders, including the law department [8]. However, indications suggest that these leaders are not as prepared as they could be to meet these threats. PricewaterhouseCoopers found that fewer than half of the chief information officers and chief security officers it surveyed "have an effective information security strategy in place and are proactive in executing the plan." The remainder lacks a strategy, fails to execute it adequately, or is essentially reactive in meeting cyber threats [9].

2- Cyber law Legislation and Guidance:

A basic definition of cyber security is "whether and how electronic data and systems are protected from attack, loss, or other compromise." It falls largely on general counsel and other senior lawyers to advice on a large scope of cyber security legal issues, including privacy concerns, data breaches, and information sharing, and developing a plan of action for potential cyber security crisis situations. Currently, data protection and privacy are governed by a "patchwork" of state and federal regulations, as well as industry-specific legislation and guidelines that can leave both large and small companies wondering where to begin [10]. More than 50 federal statutes address aspects of cyber security in some capacity, whether directly or indirectly, with no overarching piece of legislation in place. In this environment, corporate law departments naturally pay the most attention to regulations and private lawsuits, rather than federal or state legislation. Among those surveyed for this study, a majority cite regulations or lawsuits as the greatest motive for taking action, with almost equal numbers driven by internal concerns (e.g., shareholders). Substantially fewer are concerned about legislation or binding judicial precedent [11]. Although it is beyond the scope of this white paper to provide an exhaustive account of all sources of current cyber security law, the ensuing discussion outlines the major current influences in the field.



These include congressional actions of the Federal Trade Commission (FTC) Act, the SEC's disclosure guidance, and the National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cyber security [12].

3- The Role of Lawyers in Cyber security:

As the welter of laws, regulations, and policies touching on cyber security suggest, the issue has become as much a legal problem as a technical one. In the past, many companies believed that cyber security could be managed primarily by IT staff and risk management [13]. While some may still hold that belief, the question has largely shifted from whether lawyers should be involved in a company's cyber security efforts to when lawyers should become involved [14]. Lawyers are best suited to apply relevant laws to the facts and circumstances of the company, assess compliance, and inform decision-making for companies' cyber security efforts as they relate to the law. Indeed, most of the corporate counsel surveyed for this study is involved to some extent in their company's cyber security efforts, with a majority reporting that they are at least "moderately" involved [15].

CONCLUSION:

Developing countries are the most concerned with cybercrime. Lack of security can and will effectively spoil the benefits of the internet, both on an economic and governmental scale. Furthermore, failure to ensure adequate minimum security standards will negatively affect the rest of the world, and might even lead to a refusal by other countries to connect with a country, thus excluding it from the new world order. It is clear that international cooperation cannot be limited to technological considerations. Law enforcement and national security must also play a determining role. But ensuring security in cyberspace will require an international law enforcement effort. It will also be imperative that countries cooperate with each other, and that real efforts are made to assist developing countries, which often lack experience and legal knowledge on this front. It is vital that countries do not underestimate the importance of securing cyberspace if the internet is to flourish to its full capacity, bestowing its benefits on a global scale.

REFERENCES:

1. Lyons, K. "Law Firms Adding Cyber security Fields." Pittsburgh Post-Gazette, November 3, 2013. http://www.post-gazette.com/business/legal/2013/11/04/VENTURING-INTO-THE-DATA-BREACH-Law-firms-adding-cyber security-fields/stories/201311040006

2. DeMarco, J. Partner, DeVore and DeMarco. Phone Interview, July 18, 2014.

3. Sebold, J. "Cyber security Specialists in Short Supply." Los Angeles Daily Journal, August 19, 2013.

4. Bodenheimer, D. Partner, Crowell & Mooring. Phone interview. July 29, 2014.

5. Bodenheimer, D. "The Cyber Forecast – Hotter than Global Warming." Crowell and Moring, DC Cyber Security Breakfast Series, January 24, 2008. http://www.crowell.com/documents/The-Cyber-Forecast_Reviewing-2007-and-Previewing-2008.pdf

6. Pearson, H. "Cyber security: The Corporate Counsel's Agenda." Bloomberg BNA: Privacy and Security Law Report, 2012. p. 1. http://www.hldataprotection.com/files/2012/1

2/BloombergBNA-Cyber security-Pearson2.pdf

7. Fischer, E. “Federal Laws Relating to Cyber security: Overview and Discussion of Proposed Revisions.” Congressional Research Service, June 20, 2013. pp. 1-2. http://fas.org/sgp/crs/natsec/R42114.pdf

8. Client Alert: Five Things Every In-House Counsel Should Understand About the NIST Cyber security Framework.” King & Spalding Privacy & Information Security Practice Group, February 25, 2014. p. 3.

9. Joyce, S. “Congress Won't Approve Cyber security Law Until Attack Compels It to Act, Bayh Says.” Bloomberg BNA, April 7, 2014. http://www.bna.com/congress-wont-approve-n17179889411/

10. Hirsch, R. “What Every General Counsel Should Know About Privacy and Security: 10 Trends for 2014.” Morgan Lewis Webinar, March 18, 2014. p. 3. http://www.morganlewis.com/pubs/WhatEveryGCShould-Know10Trendsfor2014_18march14.pdf

11. Woods, J. “Federal Trade Commission’s Privacy and Data Security Enforcement Under Section 5.” American Bar Association Young Lawyers Division.

12. Bulleted points quoted from: “Protecting Consumer Privacy in an Era of Rapid Change: Recommendation for Businesses and Policy Makers.” Federal Trade Commission, March 2012. p. vii.

13. Lynch, S. “Experts Urge U.S. Caution on Additional Cyber Threat Disclosures.” Chicago Tribune, March 26, 2014. http://articles.chicagotribune.com/2014-03-26/business/sns-rt-us-sec-cybercrime-20140326_1_cyber-security-cyber-threat-breaches

14. Framework for Improving Critical Infrastructure Cyber security.” National Institute of Standards and Technology, February 12, 2014. p. 3. http://www.nist.gov/cyberframework/upload/cyber security-framework-021214.pdf

15. Aguilar, L. “Boards of Directors, Corporate Governance and Cyber-Risks: Sharpening the Focus.” “Cyber Risks and the Boardroom” Conference, New York Stock Exchange, New York. June 10, 2014. p. 3. http://business.cch.com/srd/Aguilar-CorporateGovernanceandCyber-Risks.pdf