Journal of Business and Economics, ISSN 2155-7950, USA
July 2014, Volume 5, No. 7, pp. 1134-1140
DOI: 10.15341/jbe(2155-7950)/07.05.2014/017

http://www.academicstar.us

Transparency and Risk Assessment Reporting: A Case Study Sector Survey of Cybercrime Disclosures

A. J. Stagliano, George P. Sillup
(Erivan K. Haub School of Business, Saint Joseph's University, Philadelphia, PA 19131-1395, USA)

Abstract: With electronic and computer crime on the rise, it is reasonable to ask how and what companies report to their shareholders about this new risk to their creation of value for owners. The U.S. Securities and Exchange Commission (SEC) recommended, in late 2011, that its registrants give careful attention to the need for disclosing costs and risks associated with cyber security. To assess the impact of the SEC guidance, this paper reports the outcome of an empirical investigation of cybercrime disclosures by the largest publicly held firms in the U.S. pharmaceutical industry. Our study encompasses firms holding about 96 percent of the industry's assets that received nearly 97 percent of its yearly revenues. We conclude that little has changed over the recent five years with respect to financial disclosure of cybercrime risks. Notwithstanding the SEC reporting guidance, registrants in this $300 billion annual sales sector seem to have ignored or disregarded the call for voluntary disclosure about cybercrime threats, risks, and costs.

Key words: cybercrime; disclosure transparency; risk assessment; SEC disclosures
JEL codes: K22, L65, M48

1. Introduction

Rapid adaptation of digital technology for financial transactions has led to an extraordinary new avenue for exploitation by white-collar villains: cybercrime. Whether it is theft of industrial secrets, employees' personal data, or customers' credit card information, high-tech crooks are the latest menace to security in the corporate arena. The global increase in computer interconnectivity has revolutionized the way organizations communicate and conduct business. Unfortunately, it also has enabled a dramatic rise in criminal activity that manipulates digital/electronic functionality for the purpose of garnering illicit gains. As with many diseconomies, costs for this negative output are difficult to calculate, internalize, or load into basic product price.

Today, we really do sit at an information *control* crossroad spot. Enormous advances in information technology have altered, in a very fundamental way, the business environment. Paradoxically, the contemporary marketplace suffers from a difficult juxtapositioning of protection for proprietary data and the profitable

A. J. Stagliano, Ph.D., Professor of Accounting, Erivan K. Haub School of Business, Saint Joseph's University; research areas/interests: corporate responsibility reporting; environmental cost financial disclosure; climate change economic impacts; cybercrime disclosure. E-mail: astaglia@sju.edu.
George P. Sillup, Ph.D., Associate Professor of Pharmaceutical Marketing, Erivan K. Haub School of Business, Saint Joseph's University; research areas/interests: business ethics; marketing in the pharmaceutical industry; healthcare insurance and reimbursement processes. E-mail: sillup@sju.edu.

leveraging of aggregations of these data. Issues raised by information security cut across two domains: individual ownership rights, on one hand, and valuable intangible assets that can be exploited—legally by corporate owners, illegally by cyber-thieves.

This is an exploratory study in an area for which there has yet to be any substantial academic research. The paper intends to evaluate the degree to which corporate entities make regulatory-body disclosures about the extent of financial risk they face from information-loss vulnerability. We report here, in an investigative manner, and on a small scale, a sector-specific empirical examination of compliance with voluntary guidelines provided recently by the U.S. Securities and Exchange Commission (SEC) to its registrants.

In the next section, the backdrop on cyber threats to information security is highlighted. Following that, additional contextual background for the empirical study is provided regarding the cybersecurity disclosure guidelines promulgated in late 2011 by the SEC. The third section below describes in detail the choice of companies, time period for study, and the method of analysis. Next, the array of outcomes from the empirical examination of regulatory filings is provided. Conclusions are drawn in the final section.

2. Background: Cyber Threats

According to the Big Four accounting firm PricewaterhouseCoopers (2009), Information is "the new corporate currency". Safeguarding that commodity would seem to be as important as protecting the dollars that constitute the standard medium of exchange.

Over the past decade, many pieces of legislation have attempted to address the management and protection of electronic data elements as well as the systems that store these items. Through statutes like the Children's Online Privacy Protection Act to control commercial online services, the Gramm-Leach-Bliley Financial Services Modernization Act that adds privacy safeguards to financial institution customer information, and the Health Insurance Portability and Accountability Act for safeguarding personal medical data, the U.S. Congress has attempted to address problems connected with electronic information vulnerability. These laws—while enunciating what appears to be a clear social directive that business entities enhance security for information that they gather/store—actually are little more than proscriptions regarding data leakage and unauthorized use.

Since the turn of the century, the whole of American society has undergone a radical information control revolution driven by technology-mediated networks. Corporate governance and operations are integrally controlled by information technology. Business communications have moved from real space to virtual space. Completely new technology-contingent business models—Amazon.com, eBay, Google, Netflix—have been introduced, evolved, and flourished. Strong corporate information security is now an essential part of the "good management" paradigm. But, have companies adapted to the new information control environment and installed adequate protections for this valuable intangible asset?

During 2007, the U.S. Government Accountability Office (GAO) conducted a major study of cybercrime. The GAO report—initially requested by the U.S. House of Representatives Committee on the Judiciary and Committee on Homeland Security—concluded that cyber threats posed a significant danger of direct negative economic impacts which ranged into the billions of dollars annually (GAO, 2007). Recognizing that affected entities face a plethora of challenges in addressing the cybercrime peril, the GAO's conclusion was that the precise cost of cybercrime is unknown because it is so rarely disclosed and reported by those impacted.

It is this conclusion by the GAO of non-disclosure that has fueled the chorus of continuing calls for enhanced personal and corporate information security. Numerous public and private entities—federal agencies, state/local law enforcement units, industry, academia—have individual and collaborative responsibilities here. But efforts, at whatever level of intensity, by these entities are impeded because cybercrimes go undetected and under-reported. The FBI estimated that in 2005 more than $67 billion of annual loss to U.S. organizations could be attributed to computer crimes (GAO, 2007, p. 16). The intangible costs due to opportunities lost by businesses from lack of consumer confidence in securing personal data is incalculable. The GAO reported that a 2007 study by the Ferris Research group estimated the global cost of spam alone exceeded $100 billion. With an estimated 15 billion daily scam pieces of e-mail distributed, it is clear that disclosure of fraudulent activities is not disclosed since the Federal Trade Commission has prosecuted fewer than 100 individuals and entities for these illicit activities (this estimate is reported by the GAO 2007 and in Matwyshyn 2005 at footnote 165). Leading up to the very recent proposals for greater security has been rejection of the presumption that no regular public accountability mechanisms for security are needed because information owners will be vigilant as a consequence of the cost of failing to do so.

3. Background: Financial Statement Disclosures

Notwithstanding the repetitive attempts by industry and consumer groups, trade organizations, legislators, and regulatory bodies, to assist in reducing information vulnerability, the existing near-epidemic of phishing attacks and hacking episodes are constant reminders of the many breaches in data security. As early as 2004 Matwyshyn, in a working paper out of Northwestern University, was advocating that the SEC mandate a disclosure requirement that addressed the issue of information leakage risks. Little was done in this area at that time—the onset of the Great Recession—since pressing issues surrounding massive financial institution and securities firm reporting failures occupied much of the regulatory mechanism.

But, significant Congressional pressure, particularly from West Virginia's Senator Jay Rockefeller, has brought about some significant progress toward shining light on cybercrime. Early in 2011, the U.S. Senate Committee on Commerce, Science, and Transportation asked the Securities and Exchange Commission to consider issuing guidance to registrants regarding their responsibility to disclose data on information security risks, including material computer network breaches and other malicious cybercrime attacks.

The SEC's Division of Corporate Finance, moving with rather unusual dispatch regarding this Congressional request, issued cybersecurity disclosure guidance on October 13, 2011. One of the most significant financial elements connected with the threat of cybercrime is the risk that these incidents have on company operations and the firm's financial outcomes. According to the SEC in its disclosure guidance document, successful cybercrime attacks create substantial economic costs and a number of other negative consequences. These untoward results include remediation outlays, increased cybersecurity protection expenditures, lost revenues, litigation threats, and reputational damages. These negative outcomes mirror the types of economic impacts first reported by the GAO in its 2007 report to Congress.

Although no extant SEC disclosure requirement explicitly recognizes a specific risk regarding cybersecurity and cyber incidents, standard reporting protocols impose an obligation on registrants to disclose such risks and incidents. Furthermore, material information regarding cybersecurity risks and occurrences of cyber-criminality

events is required to be disclosure in regulatory filings so that other disclosures are not misleading. Information, it should be noted, is considered "material" if there is a substantial likelihood that a reasonable investor would consider it important in making decisions regarding investment. This materiality filter is not necessarily confined to quantitative aspects of registrants' filings. There are both actual costs and significant, but incalculable, opportunity costs inherent in cyber theft events that compromise proprietary corporate information systems.

What does the SEC guidance propose with respect to areas of consideration for disclosure by registrants? In particular, the guidance document states that the SEC expects registrants to evaluate their cybersecurity risks—including the severity and frequency of cyber incidents during the reporting period—in light of the reporting requirements contained in Regulation S-K Item 503(c). Registrants, per the SEC guidance, also should address cybersecurity in their annual report section "Management's Discussion and Analysis of Financial Condition and Results of Operations", the so-called MD&A item. When cyber incidents materially affect the registrant's products, services, relationships with customers and suppliers, or competitive conditions, disclosure in the typical "Description of Business" item in the annual report is called for in the SEC guidance. Obviously, material pending legal proceedings stemming from cyber incidents signal a disclosure need. And, the heightened requirements of Sarbanes-Oxley providing for an assessment of the efficacy of internal control systems as they relate to cybersecurity must be considered. Ineffectiveness of disclosure controls and procedures is required reporting by all SEC registrants.

4. Case Study: The Pharmaceutical Sector

To test whether this new SEC reporting guidance had any impact on disclosures made by registrants about cyber threats and incidents, we chose to focus attention on a single industrial sector. This is new research for which there little analogous investigation has been conducted previously. Of course, there have been hundreds of sensational publications of popular-press and/or mass media reports on Internet security breaches of retail-trading corporations in the U.S during the past decade. To focus attention more closely, though, on the technical aspects of full and transparent financial statement disclosures, we have chosen to capture a single industry for very detailed examination.

In this regard, we selected the $300 billion pharmaceutical preparation and manufacturing sector that is categorized under the NAICS ("North American Industrial Classification System") code number 325412. We consider only SEC registrants that are publicly traded entities. We use year 2011—the one during which promulgation of the SEC cybersecurity disclosure guidance occurred—to assess this population group. With these parameters in place, the total number of firms available is 217.

To make the qualitative examination manageable, we chose to limit the empirical work to those firms with annual revenue of at least $500 million in 2011. Twenty-one firms met this criterion. This high sales level is hardly a "limiting" factor, since the sample of just 21 companies (not quite 5 percent of the public companies in the industry) accounts for 96.9 percent of the 2011 net revenues and 96.1 percent of the total reported industry assets. Table 1, shown below, gives the names of all the companies in the sample.

Table 1 Pharmaceutical Company Sample

AbbVie Inc. (2011 and 2012)	Eli Lilly and Company
Actavis, Inc.	Merck & Co., Inc.
Alexion Pharmaceuticals, Inc.	Mylan Inc.
Allergan, Inc.	Perrigo Company
Bristol-Myers Squibb Company	Pfizer Inc.
Cubist Pharmaceuticals, Inc.	Salix Pharmaceuticals, Ltd.
Endo Health Solutions Inc.	United Therapeutics Corporation
Forest Laboratories, Inc.	Vertex Pharmaceuticals Incorporated
Hospira, Inc.	ViroPharma Incorporated
Impax Laboratories, Inc.	Zoetis Inc. (2012 only)
Johnson & Johnson	

The relevant disclosure vehicle is each registrant's annual report, SEC Form 10-K. To determine/detect the impact on the level of disclosure that was engendered by the late-2011 SEC guidance promulgation, annual reports for three years prior to the guidance (i.e., 2008, 2009, and 2010), the issuance year, and the only additional disclosure year available—2012—are all considered. Two firms, Abbvie and Zoetis, were not stand-alone entities throughout the entire study period (see the annotations in Table 1). They are included, nonetheless, since one intention of the research is to describe the disclosure posture that exists today in the industry at a time subsequent to the SEC reporting guidance regarding cybersecurity.

The research proceeded by gathering the digital versions of five years' of Form 10-K filings for the sample companies. Ninety-eight documents were available for examination. After some careful pre-testing, we settled on a content-analytic procedure and conducted an electronic search of these documents for reporting that included any of the following seven terms[1]:

- Computer crime
- Cyber attack
- Cyber crime
- Cybersecurity
- Data leakage
- Identity theft
- Internet fraud

Search procedure "hits"—separately accumulated by year—were supplemented by identification of the actual Form 10-K item number (these are common among all SEC registrants) in which the term had been found.

5. Empirical Results: Evidence of *Non*-disclosure

The findings here are significant, but not necessarily startling. When offered the opportunity to tout "good news"—whether of a qualitative or quantitative nature—in regulatory filings, U.S. companies are well known to bask in the glow of positive reporting. On the other hand, when the only reporting is to be about costs, losses, or risks, voluntary disclosure is a very unlikely outcome. Not unexpectedly, that is precisely what we found. The outcome is marked by a nearly complete state of *non*-disclosure for the very large and important industry studied.

Given below are some of the details surrounding the empirical results. With the possibility of uncovering of

[1] Except for "Internet fraud", the search was conducted to uncover any whole-word part of these terms. Because the word "fraud" is connected so closely with required reporting on internal financial control mechanisms, only that complete phrase would indicate a specific disclosure regarding cybersecurity.

686(seven terms searched in 98 documents) disclosure references to cybersecurity, just 15 were located after an exhaustive examination. Details regarding disclosures by different companies in each year are shown in Table 2.

Table 2 Number of Companies Making a Disclosure by Year

2008	-0-
2009	1
2010	2
2011	3
2012	6

Several firms made multiple references related to cybersecurity issues in a single Form 10-K filing. All of these occurrences were in filings for 2012—the year subsequent to the SEC disclosure guidance promulgation. Table 3 shows the complete picture of the 15 disclosures found over the 5-year study period.

Table 3 Number of Separate Disclosures Found by Year

2008	-0-
2009	1
2010	2
2011	3
2012	9

As is evident from Table 2, only six of the 21 companies, a group of firms that accounted for nearly all the sales garnered and assets owned in this large industrial sector, made any mention of cybersecurity and the associated risks during the period examined.

Table 4 shows the connections between the disclosing firms and the year in which a Form 10-K filing included reference to cybersecurity issues.

Table 4 Companies Making Disclosures by Year

Allergan	2011, 2012
Bristol-Myers	2012
Hospira	2010, 2011, 2012
Mylan	2012
Perrigo	2009, 2010, 2011, 2012
Zoetis	2012

It is obvious from these tabular data that when companies first start—the initial evidence is in 2009—to mention cybersecurity, the relevant reporting on this topic continues. We might be tempted to remark that the SEC guidance prompted additional disclosure, but that would appear to be a facile conclusion to draw. Twenty sample companies existed in 2011 (Zoetis, formerly Pfizer Animal Health, was spun-off from its parent, a non-discloser, during 2013, so it has only a 2012 report from its first year of separate incorporation). Thus, *if* the SEC promulgation induced action by new reporters, only Bristol-Myers and Mylan can be considered as candidates for such stimulation actually "creating" disclosures[2]. This may be the case, but we cannot demonstrate causality, since

[2] Allowing for the potential that, notwithstanding the SEC guidance, these companies were victims of a serious/major cybercrime incident during either 2011 or 2012, we exhaustively searched the business and common public-press media for reports of such an event. We found none.

the only time we uncovered multiple uses among the seven specific search terms was by these two firms. While our research found 12 mentions (again, over a five-year period among all the sample firms) of the term "cyber attack," only Bristol-Myers reported on "cybersecurity", and only this same company, along with Mylan, used the phrase "data leakage" in its regulatory filings. So, it is to be remarked that these "new" 2012 disclosers do appear to be qualitatively better reporters.

Finally, it surely is worthwhile to round-out this discussion of the empirical results by noting that every single one of the 15 instances of cybersecurity-related reporting was found in the Form 10-K Item 1A, the "Risk Factors" section of the annual regulatory report. Although the SEC reporting guidance clearly gives examples of how registrants might be required to make qualitative disclosures in Form 10-K Item 1 ("Description of Business"), Item 1A ("Risk Factors"), Item 2 ("Properties"), Item 4 ("Legal Proceedings"), and Item 7 (the MD&A), it was only in Item 1A that any reporting occurred among our sample companies over the five years reviewed.

6. Conclusion

We have attempted here to contribute to the research literature in two areas: one related specifically to cybersecurity and the other concerned with transparency and voluntary financial-statement disclosures. It is fair to characterize this effort as an early and exploratory one. No doubt, our single industry focus adds a clear limitation for extending the outcomes beyond the niche and sector that formed the boundary for the empirical examination.

We can conclude, from this limited study, focused as it was on nearly the whole of one industrial sector, that little has changed regarding financial statement disclosure of cybercrime risks. Notwithstanding the SEC guidance, registrants are prone to ignore or disregard calls for voluntary additional disclosures in their regulatory filings. Are firms transparent with respect to the extraordinary risk of cyber-attack incidents? Not the ones studied here. Are firms full disclosers regarding the risks involved with cybercrime? Not according to what we have seen in this industry that has nearly $300 billion of annual sales.

References:

GAO (2007). *Cybercrime: Public and Private Entities Face Challenges in Addressing Cyber Threats*, GAO Report number 07-705.

Matwyshyn Andrea M. (2005). "Material vulnerabilities: Data privacy, corporate information security and securities regulation", Working Paper 524; Bepress Legal Series (March 15, 2005).

Matwyshyn Andrea M. (2005). "Material vulnerabilities: Data privacy, corporate information security and securities regulation", *Berkeley Business Law Journal*, Vol. 3, No. 1, p. 129.

Pricewaterhouse Coopers (2009). *Global State of Information Security*.

SEC (2011). Cybersecurity, Division of Corporate Finance Disclosure Guidance: Topic No. 2.