REPORTING ON THE FINANCIAL IMPACTS OF CYBERCRIME

A. J. Stagliano, Ph.D.
Professor of Accounting
Erivan K. Haub School of Business
Saint Joseph's University
Philadelphia, PA, USA

Abstract

Swift adaptation of digital technology for financial transactions has led to a 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 for business. The rapid increase in computer interconnectivity has revolutionized the way organizations communicate and conduct business. It also has enabled a dramatic rise in criminal activity that manipulatesdigital/electronic functionality for the purpose of garnering illicit gains.This research reports onthe results of an exploratory study designed to examine how publicly owned companies have responded to recent calls for disclosure about financial impacts of cybercrime.

The U.S. Government Accountability Office (GAO) conducted a major study in 2007 of cybercrime. Thereport—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 that ranged into the billions of dollars annually. Recognizing that affected entities face a plethora of challenges in addressing cybercrime, the GAO's conclusion was that the precise cost of cybercrime is unknown because it is so rarely disclosed and reported by those impacted.

The U.S. Senate Committee on Commerce, Science, and Transportation asked the U.S. Securities and Exchange Commission (SEC) to consider issuing guidance to registrants regarding their responsibility to disclose data oninformation security risks, including material computer network breaches and other malicious cybercrime attacks.The SEC's Division of Corporate Finance issued cybersecurity disclosure guidance on October 13, 2011. One of the most significant financial elements connected with the threat of a cybercrime is the risk that these incidentshave on company operations and the firm's financial outcomes. Cybercrime attacks create substantial economic costs and a number of other negative consequences. These untoward results include outlays for remediation, increased cybersecurity protection expenditures, lost revenues, litigation threats, and reputational damages.

This study seeks to determine whether firms in theU.S. retail merchandising industry—the target of recent high-profile cyber-attacks—disclose their assessment of cybercrime risks to stakeholders in annual reports filed with the SEC. Data were gathered from 2010 to 2014 Form 10-K filings for allpublically traded U.S.companies with 2010sales that exceeded $1 billion. Currently, this is a $5 trillion sector of the U.S. economy. The study group includes firms that accounted for more than half of all the revenues generated in the retail sales market.

The firms studiedall have a fiscal year enddates subsequent to October 13th,and, thus,would have known about the new SEC guidance for cybersecurity risk disclosure starting with financial reporting

for year 2011.The year prior to the SEC action (i.e., 2010) isincluded as part of the analysis so thatan assessment can be made regarding the impact of the SEC guidance announcement.

This research makes a contribution to our understanding of how firms react to non-mandated disclosure guidance that is promulgated by the SEC. Financial markets are well known to impound decision-relevant disclosures in an efficient manner. Therefore, cybercrime risk assessments provided by management in publicly available venueslike Form 10-K should assist investors in making economically rational trading decisions. The outcomes of this study help us understand the impact that SEC reporting guidance has on the voluntary disclosure posture of registrants.