DC19021

DATA BREACHES AT LARGE U.S. COMMERCIAL BANKS: EVIDENCE ON FINANCIAL STATEMENT DISCLOSURES OF CYBERCRIME RISKS AND LOSSES

Submission Information

Title: [Above; abstract following this page]

Topic areas: Accounting, Financial Reporting

Presentation format: Research paper session

Author information:

A. J. Stagliano, Ph.D.
Professor of Accounting
Erivan K. Haub School of Business
Saint Joseph's University
5600 City Avenue
Philadelphia, PA 19131-1395
Voice: 1-610-660-1652 (secretary: 1-610-660-1650)
Facsimile: 1-610-660-1126
E-mail: astaglia@sju.edu

DATA BREACHES AT LARGE U.S. COMMERCIAL BANKS: EVIDENCE ON FINANCIAL STATEMENT DISCLOSURES OF CYBERCRIME RISKS AND LOSSES

Abstract

Swift adaptation of digital technology for financial transactions has led to a new avenue for exploitation by "white-collar" villains: cybercrime. High-tech crooks are the latest menace to security in the corporate arena. 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 manipulates digital functionality to garner illicit gains.

This research reports on a longitudinal study designed to examine how certain publicly owned companies have responded to recent calls for disclosure about financial impacts of cybercrime. It documents enhanced disclosures in financial statements during the past decade.

In 2007, the U.S. Government Accountability Office (GAO) conducted a major study of cybercrime. The GAO stated that cyber threats posed a significant danger of 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/reported by those impacted.

Early in 2011, 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 on information security risks, including material computer network breaches and other malicious cybercrime attacks.

The SEC's Division of Corporate Finance, moving with unusual dispatch on this 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, successful 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 examines whether firms in the U.S. commercial banking industry—a potential target for cyber-attacks—disclose their assessment of cybercrime risks to stakeholders in annual reports filed with the SEC. Data for years 2008 through 2018 were gathered from Form 10-K filings for all publicly traded banks with 2007 deposits that exceeded $1 billion. This sample group includes firms that accounted for over half of the total 2018 U.S. commercial bank deposits.

All the firms studied have a fiscal period based on the calendar year and would have known about the SEC guidance for cybersecurity risk disclosure starting with financial reporting for year 2011. The years prior to the SEC action (i.e., 2008-10) are included as part of the analysis so that an 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. Since financial markets are well known to impound decision-relevant disclosures in an efficient manner, cybercrime risk assessments provided by management in publicly available venues like 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.

Keywords: cybercrime, cyber security, financial disclosure, reporting transparency