Chapter 5
Enhancing Cyber Security for Financial Industry through Compliance and Regulatory Standards

Derek Mohammed
Saint Leo University, USA

Marwan Omar
Saint Leo University, USA

Van Nguyen
Saint Leo University, USA

ABSTRACT

This paper investigates laws and regulations within the financial industry that are applicable to cybersecurity. It analyzes both compliance and regulatory issues across the financial sector at the federal and state levels. Additionally; the paper highlights the importance of adhering to, and implementing industry-based regulations to improve the protection of financial digital assets against cyber-attacks. It also reviews similarities and differences among compliance environments created by financial regulations. Identification, interpretation and application of federal and state government regulations, directives and acts as they apply to the security of digital systems in the financial sector is another objective of this research study. Finally, this paper contrasts the values and issues created by increasing compliance requirements.

DOI: 10.4018/978-1-5225-0741-3.ch005

CYBERSECURITY COMPLIANCE IN THE FINANCIAL SECTOR

Financial regulations provide a framework seeking to promote legal and ethical behavior within the industry. However, scandals over the last fifteen years have revealed broken regulations and poor enforcement. In each scandal's wake, lawmakers passed legislation to either amend the existing standards and enforcement mechanisms or create new. As a key pillar in a nation's economic foundation, the U.S. relies on a stable financial industry. Financial standing determines a nation's standing on the international stage. China's emergence as an international power, for example, derives partially from its economic strength.

The sheer volume of assets, the financial industry manages presents a highly lucrative target for criminals. Insiders engage in fraud, deceiving investors for ill-gotten profit, and others use complex financial systems for illicit purposes such as money laundering. Also damaging is the near-constant assault from cyber criminals. In order to protect consumers and ensure transparency, U.S lawmakers have empowered several regulatory bodies with oversight authority. Still, responsibility for regulatory compliance and safeguarding financial assets remains with individual institutions. Regulations create a diverse set of compliance environments that display some similarities, yet contain differences in focus and intent. Improving cybersecurity in the financial industry requires a critical evaluation of the merits and issues of compliance present in each environment. Only then can cybersecurity policy makers recommend regulations that promote efficiency while protecting the industry and its customers.

Analysis of Compliance Issues

Due to the financial sector's complex nature, compliance with federal, state and local laws provide a monumental challenge. Cybersecurity further complicates the issue. As former Federal Bureau of Investigation Cyber Division Assistant Director Gordon Snow (2011) explained, "Cyber criminals have demonstrated their ability to exploit our online financial and market systems that interface with the Internet." Since the financial sector depends heavily on information technology, regulatory compliance becomes a critical cybersecurity component. Because a large portion of assets exist on paper rather than physically, protecting asset data serves as a driving force for regulation.

Ensuring coherent and active cooperation with other financial entities serves as a key to achieving compliance. The Gramm-Leach-Bliley Act (GLBA), for example, dictates how institutions collect and share information. GLBA's provisions require strict confidentiality and security for personal information institutions collect, such as