Chapter XI
Role of FS-ISAC in Countering Cyber Terrorism

Manish Gupta
M&T Bank Corporation, USA

H. R. Rao
The State University of New York (SUNY) – Buffalo, USA

ABSTRACT

In recent times, reliance on interconnected computer systems to support critical operations and infrastructures and, at the same time, physical and cyber threats and potential attack consequences have increased. The importance of sharing information and coordinating the response to threats among stakeholders has never been so great. Information sharing and coordination among organizations are central to producing comprehensive and practical approaches and solutions to combating threats. Financial services institutions present highly financially attractive targets. The financial services industry, confronts cyber and physical threats from a great variety of sources ranging from potentially catastrophic attacks launched by terrorist groups or other national interest groups to the more commonly experienced extremely targeted attacks perpetrated by hackers and other malicious entities such as insiders. In this chapter we outline structure, major components, and concepts involved in information sharing and analysis in the financial services sector. Then we discuss the relevance and importance of protecting financial services institutions' infrastructure from cyber attacks vis-à-vis presentation of different issues and crucial aspects of current state of cyber terrorism. We also discuss role and structure of ISACs in counterterrorism; and constituents, functions, and details of FS-ISAC.

INTRODUCTION

The pervasive nature of the Internet coupled with recent threats of cyber terrorism makes Internet infrastructure security an area of significant importance (Devost & Pallard, 2002). Beyond isolated and annoying attacks on official Web sites, potential targets for a hypothetical cyber-terrorist act in the United States include most of the nation's critical infrastructure, including utilities such as electricity, water, and gas facilities and their

supply systems; financial services such as banks, ATMs, and trading houses; and information and communication systems (Estevez-Tapiadoe, 2004). Hacking as part of cybercrime is definitely moving forward, with new tools to hack and new viruses to spread coming out every day (Sukhai, 2004). One of the major challenges in counterterrorism analysis today involves connecting the relatively few and sparse terrorism-related dots embedded within massive amounts of data flowing into the government's intelligence and counterterrorism agencies (Popp et al., 2004). On the Internet, an attacker has an advantage. He or she can choose when and how to attack (Schneier, n.d.). However, at the operational level, how cyber terrorists plan to use information technology, automated tools, and identify targets may be observable and to some extent, predictable (Chakrabarti & Manimaran, 2002). Figure 1 shows the general framework within the operational context of financial services-information sharing and analysis centers (FS-ISAC).

In recent times, reliance on interconnected computer systems to support critical operations and infrastructures and, at the same time, physical and cyber threats and potential attack consequences have increased. The importance of sharing information and coordinating the response to threats among stakeholders has never been so great. Information sharing and coordination among organizations are central to producing comprehensive and practical approaches and solutions to combating threats. In addition, comprehensive, timely information on incidents can help federal and nonfederal analysis centers determine the nature of an attack, provide warnings, and advise on how to mitigate an imminent attack (*Homeland security,* 2003).

National critical infrastructure protection (CIP) policy for the United States as covered in Presidential Decision Directive (PDD) 63 and confirmed in other national strategy documents, including the *National Strategy for Homeland Security* issued in July 2002, called for a set of strategies and actions to establish a partnership between the public and private sectors protecting national critical infrastructure. For these sectors, which now total 14, federal government leads (sector liaisons) and private-sector leads (sector coordinators) were to work with each other. Federal CIP policy also encourages the voluntary creation of information sharing and analysis centers (ISACs) to serve as mechanisms for gathering, analyzing, and appropriately sanitizing and disseminating information to and from infrastructure sectors and the federal government through NIPC (*Homeland security*, 2003). ISACs, today, control over 80% of nation's critical infrastructures.

The financial services industry, confronts cyber and physical threats from a great variety of sources ranging from potentially catastrophic attacks launched by terrorist groups or other national interest groups to the more commonly experienced extremely targeted attacks perpetrated by hackers and other malicious entities such as insiders. A concerted, industry-wide effort to share attack information and security best practices offers the best hope of identifying, responding to, and surviving the very real threats facing both the industry and the country (*Financial service-information sharing and analysis centers (FS-ISAC) brochure*, n.d.).

In this chapter we outline structure, major components, and concepts involved in information sharing and analysis in the financial services sector. Then we discuss the relevance and importance of protecting financial services institutions' infrastructure from cyber attacks. The next section elaborates and illustrates information sharing as a key element in developing comprehensive and practical approaches to defending against potential cyber and other attacks. In following section, we present different issues and crucial aspects of current state of cyber terrorism. Then, we discuss role and structure of ISACs in counterterrorism, using information sharing as an operational tenet. Next we discuss, in detail, constituents, functions, and details of FS-ISAC. The final section concludes the chapter with a summary and discussion.

Social Engineering Techniques and Password Security: Two Issues Relevant in the Case of Health Care Workers
B. Dawn Medlin (2013). *International Journal of Cyber Warfare and Terrorism (pp. 58-70).*
www.irma-international.org/article/social-engineering-techniques-and-password-security/101940