Abstract  Information security management is becoming a more critical and, simultaneously, a challenging function for many firms. Even though many security managers are skeptical about outsourcing of IT security, others have cited reasons that are used for outsourcing of traditional IT functions for why security outsourcing is likely to increase. Our research offers a novel explanation, based on competitive externalities associated with IT security, for firms’ decisions to outsource IT security. We show that if competitive externalities are ignored, then a firm will outsource security if and only if the MSSP offers a quality (or a cost) advantage over in-house operations, which is consistent with the traditional explanation for security outsourcing. However, a higher quality is neither a prerequisite nor a guarantee for a firm to outsource security. The competitive risk environment and the nature of the security function outsourced, in addition to quality, determine firms’ outsourcing decisions. If the reward from the competitor’s breach is higher than the loss from own breach, then even if the likelihood of a breach is higher under the MSSP the expected benefit from the competitive demand externality may offset the loss from the higher likelihood of breaches, resulting in one or both firms outsourcing security. The incentive to outsource security monitoring is higher than that of infrastructure management because the MSSP can reduce the likelihood of breach on both firms and thus enhance the demand externality effect. The incentive to outsource security monitoring (infrastructure management) is higher (lower) if either the likelihood of breach on both firms is lower (higher) when security is outsourced or the benefit (relative to loss) from the externality is higher (lower). The benefit from the demand
externality arising out of a security breach is higher when more of the customers that leave the breached firm switch to the non-breached firm.

15.1 Introduction

Information security management is emerging as a critical business function, partly because of firms’ increasing reliance on the Internet to conduct business and increasing regulatory requirements. Simultaneously, information security management is becoming more complex and challenging. Some of the reasons for this include changes in attack patterns over time (increased frequency, severity and sophistication of attacks); complex information technology (IT) environments consisting of multitudes of hardware, operating systems, application software, and distributed networks, each with its own vulnerabilities; shortage of security professionals with the required expertise; diverse security solutions from vendors; limited IT budgets; and demanding audit and regulatory requirements (e.g., Sarbanes Oxley (SOX), California Senate Bill No. 1386, Gramm-Leach-Bliley Act (GLBA), Health Insurance Portability and Accounting Act (HIPPA), Payment Card Industry Data Security Standard (PCI DSS), Basel II, among others). Outsourcing to Managed Security Service Providers (MSSP) has emerged as one of the key strategies to deal with the complexities of IT security management. The MSSP industry is relatively new, but analysts project significant growth in the MSSP industry. According to IDC, the value of U.S. managed security services market was approximately $1.3 billion in 2007, an increase of 19.6% over 2006; this figure is expected to reach $2.8 billion by 2012 [21]. Yankee Group [29] estimated that the global spending on managed security services was approximately $4 billion in 2006. They projected managed security services market to grow at a compound rate of 14 percent from 2006 through 2010. Frost and Sullivan [15] projects that managed security services will exceed $6 billion by 2011. According to Gartner, in 2006, 60% of Fortune 500 enterprises had used an MSSP, and about 20% of enterprise firewalls were under remote monitoring or management [23]. The range of services outsourced includes perimeter protection which includes managed services for firewalls, IDSs, VPNs, and other security infrastructure management, security event monitoring, incident management including emergency response and forensic analysis, and security consulting that includes vulnerability assessment, penetration testing, network architecture review, and compliance gap analysis.

Even though many security managers are skeptical about outsourcing of IT security [28], [14], mainly due to the fear of losing control over sensitive information, industry analysts have cited cost savings, better protection, leveraging of expertise, economies of scale, compliance with laws, and liability transfer as the primary drivers for the outsourcing of information security functions [42], [10], [33]. Schneier [34] noted that information security is part of IT infrastructure and “infrastructure is always outsourced”. These reasons for IT security outsourcing suggest that practitioners and industry experts do not view IT security as different from tra-