Chapter 7
An Information Governance Model for Information Security Management

Matthew Nicho
University of Dubai, UAE

ABSTRACT

The purpose of this paper is to propose an IS security governance model to enhance the security of information systems in an organisation by viewing security from a holistic perspective of encompassing information security, information assurance, audit, governance, and compliance. This is achieved through the strategic integration of appropriate frameworks, models, and concepts in information governance, IS service management, and information security. This involves analysing the relevant frameworks, models, and concepts used in the above domains, extracting the best practices for implementing them from the literature and mapping these into an integrated standard. The frameworks identified are Control Objectives for Information and related Technology (COBIT), Information Technology Infrastructure Library (ITIL), ISO 27002, Risk IT, and Payment Card Industry Data Security Standard (PCI DSS). While it is evident that each of these five frameworks serve different purpose of information systems, such as information auditing and governance, facilitating the delivery of high-quality IT services, providing a model managing an Information Security Management System, providing a risk focus, and protection of cardholder data, all of these frameworks have the common objective to secure the IS assets in an organisation. Hence, extraction of the best practices in each of these framework can provide effective security of organisational IS assets rather than adequate security.

DOI: 10.4018/978-1-4666-2083-4.ch007

INTRODUCTION

IS security has become a critical concern facing modern organisations today considering the fact that organisations are fully dependent on IT for survival. This is compounded by the fact that more confidential information is stored in remote servers on the Internet. During the first half of 2011, there had been a number of high profile and persistent IS security breaches in organisations namely Sony, the data-security firm RSA, Lockheed Martin, the email wholesaler Epsilon, the Fox broadcast network, NASA, PBS, the European Space Agency, the FBI, the British and French treasuries, the banking and insurance giant Citigroup, along with dozens of other companies and government agencies (Liebowitz, 2011).An analysis of these reveal that if a few non-technical procedures were followed in most of these breaches (RSA, Sony and Epsilon see Exhibit 1) these breaches could have been avoided. The data breach at RSA, Sony and Epsilon occurred due to spear phishing rather than highly sophisticated hacking. According to a key manager at RSA technological advances in IS security and the use of IS security controls/frameworks, and compliance on IS security regulations could have prevented the IS security breaches to a great extent. Despite these improvements over the years, there has been no reduction in the rate of attacks on information systems. According to the Identity Theft Resource Center (ITRC, 2011), hacking accounted for the largest number of breaches in the first quarter of 2011 as almost 37% of breaches were due to malicious attacks on computer systems which is more than double the amount of targeted attacks (17.1%) reflected in the 2010 ITRC Breach List. This necessitates a review of IS security controls available and employed, analyse the gaps in the IS security frameworks to propose a holistic perspective of information security governance. The high profile breaches during the first half of 2011 (see Exhibit

Exhibit 1. A case of a provider of security becoming a victim

RSA started in 1982 is a division of EMC Corp that provides security, risk, and compliance solutions for businesses and according to the company, it is chosen by more than 90% of Fortune 500 companies for managing there is security. In fact, RSA is the inventor of the public key cryptographic algorithm that enable secure transparent exchange of encrypted communications between users and enterprises on the Internet. They provide technology and business solution for managing IS security, provide strong two-way authentication, access control, data loss prevention solutions. They also provide encryption, tokenization and GRC solutions, along with a host of other security solutions.

On March 17th 2011 the company disclosed to the Securities and Exchange Commission that a data breach has occurred. Unlike other data breaches, no customer data like email addresses, usernames, credit card numbers, date of birth or social security numbers were stolen. The attackers used a common form of phishing called spear phishing. In this type of attack, the attacker sent two different phishing emails over a two-day period. The two emails were sent to two small groups of lower level employees with the email subject "2011 Recruitment Plan."The email went to the junk folder but one employee retrieved it from their Junk mail folder, and open the attached excel file. It was a spreadsheet titled "2011 Recruitment plan.xls. The spreadsheet contained a zero-day exploit that installs a backdoor through an Adobe Flash vulnerability (CVE-2011-0609). (Adobe has immediately released a patch for the zero-day, so it can no longer be used to inject malware onto patched machines).

The attacker then proceeded to install a remote administration tool that allows the attacker to control the machine. The tool used for this was a variant of Poison Ivy set in reverse-connect mode that makes it more difficult to detect. In this reverse connect mode the victim machine reaches out and connect to the command and control rather than the other way around where the attacker machine connect to the victim machine. Once this was set up,the attacker started digital shoulder surfing to establish the employee's role and their level of access. In this mode, the attacker is in a position to escalate the user privilege; they could discover valuable data sources and extract them to external rouge servers. In this case sensitive information from more than 40 million employees may have been compromised. The estimated cost to the company by various sources is $ 66 million in direct and attributable costs.

Spear phishing is a type of attack using the Advanced Persistent Threats (APT), where the attacks are targeted at individual employees rather than the organisational security defenses. One simple flaw or overlook of the employee is all needed for en entry inside these defenses. When it comes to APTs it is not about how safe, secure and good the company is, but that a totally new approach for entering the organization is selected where the attacker don't bother to hack the organization and its infrastructure, rather focus on hacking the employees.

(Source: Adapted from the 'Anatomy of an Attack' by Uri Rivner from the website http://blogs.rsa.com/rivner/anatomy-of-an-attack/*)*