Chapter III
Impact of the Human Element on Information Security

Mahi Dontamsetti
President, M3 Security, USA

Anup Narayanan
Founder Director, First Legion Consulting, India

ABSTRACT

This chapter discusses the impact of the human element in information security. We are in the third generation of information security evolution, having evolved from a focus on technical, to process based, to the current focus on the human element. Using case studies, the authors detail how existing technical and process based controls are circumvented, by focusing on weaknesses in human behavior. Factors that affect why individuals behave in a certain way, while making security decisions are discussed. A psychology framework called the conscious competence model is introduced. Using this model, typical individual security behavior is broken down into four quadrants using the individuals' consciousness and competence. The authors explain how the model can be used by individuals to recognize their security competency level and detail steps for learning more effective behavior. Shortfalls of existing training methods are highlighted and new strategies for increasing information security competence are presented.

KNOWLEDGE & INFORMATION SECURITY

We live in an information age. Companies that are successful are those that are able to harness and utilize information to their competitive advantage. Along the same lines, economies and countries that are successful in this age are the ones who are networked; information based and those who empower their population. The electron (information based economy) has replaced the atom (nuclear power) as the true indicator of

strength of a country. Given the wide spread and critical nature of information, protecting information, that is, information security, is essential for maintaining competitive advantage and business sustenance.

The threats to information are varied. They are technical, physical, and human in nature. To counter these threats, information security has evolved over the past few decades. We are today, in the third generation (3G) of information security. It has evolved from its initial focus on technology, to its focus on processes (standards, best practices) and to the current focus on the human element that manages or uses the technology and processes.

The shift in focus from technology to processes, and subsequently the human element, has come with the realization that technology and processes are only as good as the human beings that use them.

The evolution of the information security model has occurred due to the evolution of the type of threats that businesses are faced with on a day-to-day basis. The threats have evolved and become more sophisticated. Typical threats that occurred during the technology implementation phase were viruses, worms, distributed denial of service (DDOS), and so forth. Use of firewalls, anti-virus, and IPS systems grew as a means of countering those threats. Human element related threats during this phase were device misconfigurations, excessive trust in security technology, and security flaws within the technology itself. For example, attitudes like, "I have this anti-virus, so I am secure, now let me look at other non-security issues" were common place. The other major problem was security flaws within the technology itself. For example, security flaws within the software that were installed in firewalls, anti-viruses, and so forth.

Typical threats during the process implementation phases were: too much reliance on documentation and absence of actual practice. This phase does justice to the saying "documented but not practiced." For example, organizations invested time and money in documenting policies, processes for information security, especially during the periods of legal regulations and compliance. The result was that there were numerous documents that helped the organizations to comply to legal regulations but did not substantially reduce information security risk.

The main reason why technology and processes have not managed to effectively bring down the instances of information security incidents is because the people entrusted with managing the technology and processes were not motivated, aware, responsible, and qualified for information

Figure 1. Evolution of information security