Chapter 2
Mitigating the Blended Threat: Protecting Data and Educating Users

Christophe Veltsos
Minnesota State University, Mankato, USA

ABSTRACT
While technological controls such as anti-virus, firewall, and intrusion detection, have been widely used to mitigate risk, cyber-attackers are able to outsmart many such controls by crafting new and more advanced malware and delivering them via planned attacks, a perfectly blended threat. This chapter explores this evolving threat and the failure of traditional controls. New strategies are presented to address this new threat landscape, including both human and technological approaches to mitigating risks of doing business in a Web 2.0 world.

INTRODUCTION
In early January 2010, Google shocked the world by revealing that it had been hacked. Just a month earlier, hackers had penetrated Google’s systems to steal intellectual property as well as data about some of its Gmail service users, notably human rights activists (Google, 2010; Zetter, 2010). The event was not an isolated case, however, and reports quickly surfaced that as many as 20 other large U.S. companies had been similarly probed and breached, including some outside the technology sector such as companies in the finance and chemical sectors. The attacks were targeted with pinpoint accuracy and the attackers had successfully penetrated the technical defenses in place at some of the most technologically and security savvy companies.

Financial sector companies, a lucrative target for attackers, have also had their share of security incidents. In early 2009, Heartland Payment Systems announced that its computer systems had suffered one of the largest data breach ever, potentially exposing as many as one hundred and
Mitigating the Blended Threat

thirty million credit card transactions (Worthen, 2009; DatalossDB, 2010). The level of sophistication of the attack was termed “light-years more sophisticated” (Zetter, 2010) than commonly seen malevolent activity. The malware was so deeply rooted that an earlier investigation by internal employees and regular audits had not been able to detect its presence. In March 2010, one of the masterminds behind the attack was convicted to 20 years in jail for his role in the breach. Yet, this was only one in a string of massive breaches perpetrated by the same small group of attackers, who, according to the indictment, would “identify potential corporate victims, by, among other methods, reviewing a list of Fortune 500 companies” (US-DOJ, 2010, p. 6). The list of companies infiltrated by this group reads like a who’s who of large businesses. For Heartland however, the costs of dealing with the aftermath of this incident are still mounting. According to the company’s Q1-2010 SEC filings, it has spent upwards of 139 million dollars to deal with the “processing system intrusion” (US-SEC, 2010).

However, attackers are not solely focused on large, well-funded targets. Any business that has something of value—be it financial, intellectual, military or healthcare data—can find itself a target. Furthermore, the continued decentralization of IT infrastructure means that there are more systems to be secured and sensitive data is likely to flow all throughout the enterprise and beyond with the use of Web 2.0 technologies. Meanwhile, information security professionals have the arduous task of ensuring the confidentiality, integrity, and availability (CIA) of data across the enterprise, using a combination of physical, technical, and administrative controls. Yet, these professionals have come to realize that many of the technologies that work today to protect the company may no longer be effective tomorrow. The need to continuously adjust one’s security measures is due not only to the rapid adoption of new technologies but also to the rapid rate of innovation shown by attackers. Attackers are able to exploit new vulnerabilities almost as soon as existing ones are being patched, creating a constant game of cat and mouse between security professionals and attackers.

As companies embrace the benefits of Web 2.0—a term used broadly to include rich Internet-based applications, Software As A Service, and Cloud Computing—new opportunities are created for attackers to try to acquire, modify, or destroy company data. As explained in more details in the sections that follow, current technological controls have so far proven quite ineffective in countering these new and rapidly evolving threats. Existing policies must be updated, or new ones created, and practices must be adjusted to ensure continued safety and privacy of sensitive data. To date, a company’s best tactic in protecting sensitive data is the adoption of appropriate technical controls combined with the education of its workforce about the risks posed by a Web 2.0 world.

The failure of existing technical controls to provide adequate protection against these threats puts greater importance on hardening systems that handle sensitive data, developing an incident response capability to deal with incidents that are likely to arise, and developing more effective information security education, training, and awareness programs (SETAs). While SETAs need to be periodically revised in order to stay current with company policies and practices as well as the ever-changing nature of threats, management also needs to evaluate and validate the effectiveness of SETA programs, rather than simply counting the percentage of employees who have completed the annual awareness training.

CYBER-CRIME: A CLEAR AND PRESENT DANGER

In less than a decade, business executives, government leaders, and citizens everywhere have come to realize the rapid rise of a new problem, one with global actors and victims: cyber-crime.