Marketing Vulnerabilities in an Age of Online Commerce

Robert S. Owen
Texas A&M University, USA

INTRODUCTION

This article provides an overview of strategic and tactical threats to the marketing efforts of businesses engaged in online marketing activities. Marketing-related assets that are vulnerable to attack include networking and hardware resources, human resources, information resources, promotion resources, and brand equity and customer good will. Vulnerable areas that an organization should protect include its core network and computing infrastructure, its internal social infrastructure, domain name registrations related to its branding, and branding exploits on external social networks. Although hacks of networking and hardware resources are of concern, the focus of this article is on encouraging marketing managers and strategists to consider a wider variety of external and internal threats.

BACKGROUND

While the Internet has provided new opportunities for businesses and marketing, it has also created new vulnerabilities to attack. An organization's existing brand name can be taken hostage or destroyed via the online activities of third parties; opportunities to penetrate an online market with a new brand name can be diminished or eliminated by the actions of external third parties. Customer good will can be destroyed by the online activities of competitors or disgruntled customers. Technical, financial, and human resources can be diluted or consumed by the online activities of third parties. Confidential internal information can be compromised by employees who use email and social networking websites for non-mission or personal uses.

This article attempts to outline such emerging strategic and tactical threats to online marketing efforts. While technical support people tend to focus on threats to hardware and networks, little guidance exists for marketing managers who should be interested in a wider variety of issues that can affect an organization's products, promotion, distribution, and costs (which affect pricing). "Scholarly" discussion on the subject is almost non-existent, so this article attempts to compile, categorize, and discuss the sorts of issues that are starting to emerge in the popular press.

STRATEGIES AND TACTICS FOR ATTACK

The following are emerging strategies and tactics for competitive attack that have been enabled by online technology.

Harvesting an Organization's Information Resources

Information is an asset that an organization uses to competitively design, build, promote, and distribute products. A survey by the Ponemon Institute found that the average cost in the US for *each* data record breached was $194 in 2011, including the cost of lost current and future customers (Poneman Institute, 2012).

There are three basic ways for an outsider to gain access to an organization's information resources: through exploits of the networking infrastructure, through exploits of the human social network, and through human mistakes. Networking exploits to obtain internal information could include system scans and probes, account and root compromises, packet sniffing, and malicious programming (cf. NIAC, 2004). The 2010/11 CSI Computer Crime and Security Survey (Richardson, 2011) reports that in 2010, 29% of respondents had experienced attacks through network bots, 16% denial of service attacks, and 11% password sniffing.

DOI: 10.4018/978-1-4666-5888-2.ch533

Attempts to fish for information do not have to be aimed directly at scanning and probing a networking system from the outside environment, however. The 2010 Computer Crime and Security Survey also reported that 67% of respondents had experienced attacks through malware (malicious programming). A *remote access Trojan* is a hidden piece of malicious software that is attached to another seemingly innocent software application, such as a cute electronic greeting card or a more serious looking Excel spreadsheet (Panda & Mangla, 2010; Vamosi, 2004). When these executable applications (greeting card, screen saver, spreadsheet, etc.) are opened, the Trojan is silently released to begin, say, covertly scanning files or logging keystrokes to be silently sent to another organization. These can be injected into an organization's computer if an employee opens an infected email message or if an employee brings work that was infected on an online home computer. Once inside the organization, the Trojan can attach itself to internal applications that are exchanged, such as when employees exchange internal email with executable attachments.

Microsoft employees, for example, reportedly received an infected email which released a Trojan inside the Microsft organization; this in turn disguised itself as the Notepad text editor and sent information to a remote computer in Asia, with stolen passwords then used to gain access to the source code of Microsoft products (Thurrott, 2001). Attempts to fish for information can be targeted to individual high-level executives, not just the organization as a whole. For example, an individual who opens an Excel spreadsheet attached to an email message could unknowingly be installing a malicious program that now scans that person's files for information that is sent back to the criminal hacker (cf. Miller, 2007).

Information can be lost to unauthorized third parties through the loss of a physical devices in the possession of employees or partners. Apple has experienced the loss of prototype iPhones on more than one occasion, resulting in online descriptions of products that had not yet been introduced to the public and online photographs of disassembled product internals for competitors to see. Apple described the value of one lost iPhone 4 prototype as "priceless" (Dilger 2011).

Perhaps more common, information can be released electronically through the mistakes or ignorance of employees. Members of the British Computer Society were sent a customer satisfaction survey that mistakenly contained the email addresses of all recipients in the "to" field, allowing recipients to see the addresses of all other members (Oates, 2007). Information can also be obtained through simple employee ignorance. For example, employee names and email addresses can be harvested through the use of *chain email* (also known as a chain letter). Chain email relies on *social engineering*, whereby one employee receives an email message, e.g., describing a cute lost puppy looking for a good home, and feels compelled to forward it to others within and outside of the organization. As each recipient forwards the seemingly harmless message to several others, a name and address list can be accumulated in each forward. This list can then be harvested when the chain letter eventually makes its way back out of the organization to the perpetrator; this allows a competitive intelligence researcher to find out who is employed by the organization, to find out who are partners or affiliates with the organization, or to find out who are the less-careful employees who are more likely to open email of malicious intent. One of the more well-known incidents is the "Richard Douche Free CD" chain letter, in which the perpetrator offered a free CD to anyone who forwarded it to others with a CC to the perpetrator (Hoaxbusters, undated a).

Another way to harvest email addresses is to send a message that contains a single unseen one pixel image tag. If the email is received and opened, the hidden link accesses an external server and a record that this is a live email address is made. The sender merely needs to guess at email addresses and to use a subject line that is either motivating (social engineering) or appears to be official business in order to get a recipient to open it. The simple method of implementing this tactic is described by Voicenet Communications (undated). Organizations can use email clients that block images, but this in turn creates problems for marketers (e.g., suppliers and other business partners) who send email with legitimate product images (cf. Popov and McDonald, 2004).

Disruption and Consumption of Network and Hardware Resources

Disruption and consumption of networking and computing resources can temporarily inhibit an organization from conducting online commerce (cf. CERT, undated). Gordon et al. (2005) reported that annual business fi-