JULY 2010

PRIVACY LAW ALERT

from the Privacy & Information Security Group of Poyner Spruill LLP

"Avon calling…" (or is it)? A few reasons to get prepared for social engineering

the new art of parting your organization from its critical information.

by Elizabeth Johnson

When summer hits full swing, you can always count on the tried and true activities that are the hallmarks of these warmer months. School is out, families are embarking on vacation, beachgoers are frying in the sun, and thousands of hackers are preparing to converge on Vegas for arguably the world's largest hacker conference, DEF CON, during which they often wreak a little havoc on the private sector in the name of fun and raising awareness of security flaws.

Is getting hacked not on your list of typical summer fun? Well, to see how you can avoid it, let's consider just one of this year's DEF CON events, billed as a "capture the flag" contest. This contest is a bit lower-tech than you might expect. Rather than hunching over a laptop, cracking a sophisticated computer code to gain access to information systems, this year's participants need only pick up a phone and engage in "social engineering." In short, the contestants will be showing off their social engineering prowess by calling the target organization and using all their powers of deception and coercion to extract (within 20 minutes) as many "flags" as possible from the unlucky person who answered the phone. The flags are specific items of information, selected in advance by contest organizers. Who is the target? The unfortunate targets have been selected from among contestant suggestions and so could be any organization except (as DEF CON wisely suggests) government agencies or defense contractors. For more on the rules and particulars, visit the contest site.

The first place winner receives a specially branded 16GB iPad and bragging rights. The only "loser" of this contest is the target company, which, in the best case, has a little egg on its face or, in the worst case, suffers bad press and a potential information security breach.

So what to do? Well, you might consider not answering your office phone from July 30-August 1 when DEF CON takes place. You also could cross your fingers and rely on the presumably very low probability that your organization was chosen as a target. But odds are, sooner or later, someone with malicious intent will target your organization, and they may not have the same "fun" motives as DEF CON, which actually does aim to avoid serious damage and legal violations in its contests. My advice is to use eye-catching events like this as an example to management of why appropriate privacy and information security training is not only appropriate but critically necessary to protect your organization from "attacks" that are now virtually inevitable. A hacker conference may not be the most practical example, but it is one among an amazing diversity of malicious activities that are striking organizations with increasing frequency. Being proactive to raise awareness is quite possibly the most effective defense against these attacks.

This particular DEF CON contest gives you an opportunity to consider and address your organization's preparedness to deal with one type of attack: "social engineering," loosely defined as "the act of manipulating people into performing actions or divulging confidential information …typically appl[ying] trickery or deception for the purpose of information gathering, fraud, or computer system access." This type of attack can come in many forms, such as phishing emails (like those emails that appear to be from a legitimate sender but contain malware or a link to a malicious website), spoofing calls (in which caller ID readouts are "tricked" into presenting the ID of legitimate callers, like your own IT department) or just plain old deception that can be conducted by phone, email, text or instant messages; via online chats or social networking; and even in person. Helping your employees to understand the methods and sources of these attempts to gain access to personal or corporate information and systems will help you better-secure your organization, addressing the "human error factor" that your technology controls are incapable of entirely blocking

Elizabeth Johnson's practice focuses on privacy, information security, and records management. She may be reached at 919.783.2971 or ejohnson@poynerspruill.com.

p.s. Poyner Spruill LLP
ATTORNEYS AT LAW