

An Analysis of the Hewlett Packard Investigation from a Social Engineering Perspective

A Brief History

In 2005, Hewlett Packard (HP) began an investigation into unauthorized leaks to the media concerning sensitive HP business practices. These leaks were believed to be coming from within the HP Board of Directors.

In the course of the investigation, HP employed a tactic known as **pretexting** (using the telephone under false pretenses to fraudulently obtain information). HP utilized pretexting to obtain **personally identifiable information**, or **PII** (any piece of information which can potentially be used to uniquely identify, contact, or locate a single person.) At the core of the HP issue is the fact that HP *intentionally and fraudulently* accessed information that the law defines as private, specifically telephone records.

Some examples of PII include:

- Name (if considered uncommon)
- Address (physical or email)
- Personal Telephone number
- Social Security Number
- Driver's license number
- Date and location of birth
- Financial or Credit Card account information
- Medical Information
- Biometric information, such as face, fingerprints, or handwriting

Some examples of information that might be considered PII by some, but actually is not:

- Information that is collected anonymously
- First or last name, if common
- Country, state, or city of residence
- Age
- Gender
- Race
- Name of school the individual attends or workplace of individual
- Grades, salary, or job position
- Usernames and passwords

HP's investigation was focused on obtaining PII of specific individuals, including board members, journalists, and employees. HP did not perform a broad assessment of their organization as a whole, or even of a business unit within the organization. Instead, they targeted some likely sources of the leaks, and fraudulently obtained PII related to those individuals. This was not part of an overall security audit. In fact, HP President and Chief Executive Officer Mark Hurd called the scandal the result of a "rogue investigation."

What Does the Law Say About Pretexting?

Pretexting, while not a new tactic, is relatively new to the law. There are few laws that currently address the issue specifically. A number of laws address the privacy rights of individuals, and extrapolations can be made to apply to pretexting. A brief overview of some of the laws that directly or indirectly discuss pretexting follow:

1. Gramm-Leach-Bliley Act

The Gramm-Leach-Bliley Act of 1999 (GLBA) was enacted to bring forth a number of major changes in the way the financial and insurance industries are regulated. The Privacy Rule section of GLBA goes into great detail to discuss the efforts that must be made to protect the privacy and security of the consumer's PII. Pretexting is specifically mentioned as an illegal method of obtaining PII. GLBA essentially states that all PII must be used strictly for legitimate business purposes, and it must also be protected from loss, theft, hackers, and Social Engineers.

2. Sarbanes-Oxley Act

Sarbanes-Oxley (SOX) was passed in 2002 in response to a number of very high profile accounting scandals affecting a few major corporations. SOX applies to all publicly traded companies. SOX was designed to make the financial and accounting processes of companies transparent.

SOX has a heavy emphasis on information security. SOX addresses several key components of IT security, including:

- Risk assessments,
- Implementing internal controls,
- Security awareness and training,
- Documenting security processes,
- Auditing information security,
- Ensuring physical security of information systems.

While SOX does not specifically mention pretexting, the implication is clear that companies are required to defend against the technique.

As a result of the HP issue, Congress has a number of pending bills which relate specifically to pretexting. Most of these bills focus on obtaining phone records. Among these are:

1. HR 4127 (Financial Data Protection Act of 2006)

To protect consumers by requiring reasonable security policies and procedures to protect computerized data containing personal information, and to provide for nationwide notice in the event of a security breach.

2. HR 4662 (Consumer Telephone Records Protection Act of 2006)

To prohibit the obtaining of customer information from telecommunications carriers by false pretenses, and the sale or disclosure of such records obtained by false pretenses.

3. S 2177 (Consumer Telephone Records Protection Act of 2006)

To make the stealing and selling of telephone records a criminal offense.

How a Social Engineering Assessment is Performed by RocketReady

RocketReady's Social Engineering vulnerability assessments are performed under very strict guidelines. These guidelines are developed between RocketReady and the client. All assessments performed by RocketReady are guided by several core philosophies:

1. **RocketReady always performs its assessments in an ethical, professional, and authorized manner.** RocketReady clearly defines its techniques with the client and does not stray from those authorized techniques. RocketReady uses methods that a Social Engineer would use, but with the goal of locating areas of vulnerability, weaknesses in policy, and potential breaches in information security.
2. **RocketReady never intentionally attempts to access PII or other private information, such as phone records, through deception or any other means.** RocketReady does not access PII through pretexting or email phishing. In some instances, PII is found in public locations (such as through an Internet search), but this information is not used to determine the identity of any specific individual.
3. **RocketReady performs vulnerability assessments, not investigations.** RocketReady never attempts to target an individual, or group of individuals in an effort to uncover an impropriety. Instead, RocketReady attempts to gain an overall understanding of the security posture of a company, or a sub-set of the company. No specific personnel are targeted for assessment or impersonation.

RocketReady typically has three major components of the assessment portion of its services:

1. **Phone Assessment:** Using Social Engineering techniques in an attempt to determine the level of vulnerability that exists within the organization to a phone attack. Vulnerabilities are noted with employee behavior as well as the parameters of the phone system itself.
2. **Electronic Assessment:** Using email phishing and fraudulent websites to determine the level of vulnerability within the organization to an email attack. Typically, phishing emails only solicit username and password information.
3. **Physical Assessment:** Attempting to gain access to the organization through physical entry, or to the network through a physical device. To gain access to a facility, RocketReady personnel will use several means, from simply asking for access to attempting to enter under false pretenses. To gain access to the network through a device, RocketReady might plant (or give out) CDs or USB Drives to see if employees are willing to attach these devices to their work computer. A Social Engineer will use these devices to surreptitiously gain access to the network or spread a virus throughout the network.

The Importance of Assessing the "Human Side of Security"

Corporations have a responsibility to protect the sensitive information they maintain.

This information may include:

- Consumer medical information,
- Consumer financial or credit information,
- Personnel records,
- Telephone records,
- Proprietary corporate information,
- Classified or highly sensitive information.

Laws such as GLBA and SOX, as well as a number of pending bills all clearly state that corporations must proactively protect this information from theft or loss. To do this, corporations must:

- Perform routine network penetration tests to determine weaknesses within the network architecture,
- Perform routine Social Engineering assessments to determine vulnerabilities that exist within personnel of the organization,
- Develop policies, procedures, and technical specifications that safeguard the organization's network and employees,
- Perform ongoing training to educate employees of their roles and responsibilities as they relate to information security.

A recent study reported on the Consumer Affairs website* revealed that of the 126 companies surveyed, over 54 percent lost data or suffered a breach due to employee error, with 34 percent being due to outside hackers or other intrusion attempts, and the rest due to other causes. The study's author concluded, "All of sudden, employers are realizing that the biggest security threat they face to the sensitive data they are storing and/or sending is now coming from employees who can't get caught by the millions of dollars of security technology designed to prevent the bad guys from getting in." This statistic, coupled with statements such as the Gartner Group declaration that "*Social Engineering is the single greatest security risk in the decade ahead,*" make it clear that corporations must invest in efforts to assess their personnel in order to determine exactly what vulnerabilities to information security exist, and how they can be mitigated.

* http://www.consumeraffairs.com/news04/2006/06/data_breach_audit.html