Welcome back WIU students & faculty. Our security awareness efforts are expanding to the web. See the full September Security & Privacy News newsletter at http://www.wiu.edu/universitytech/securitySpecial/techSecurity/awareness.php.

I Know What You Did Last Summer

Like the 1997 movie by the same name the September Technology Security & Privacy newsletter topic "University sensitive data handling" is a horror story of sorts. It began harmlessly enough on a cold damp day in late May as University Technology (uTech) implemented a new anti SPAM solution. Part of that solution gave the university a window from which to begin to understand the use of Credit Card and Social Security numbers (SSNs) coming across unprotected in university email.

"The truth will set you free. But first, it will piss you off" – Gloria Steinem

Statistics gathered over the summer, while painful to observe, are important to understand and to build upon:

- **133** full credit card numbers and **20** CVV2/CVC2/CID numbers (security code on the back of your credit card) were found
- **1,787** SSNs were found

That is approximately two credit card numbers and thirty SSNs discovered each and every business day (and one credit card security code discovered every third business day) via unprotected email. It is likely that these numbers would be even higher during the school year.

Oh, so this is a bad thing?

Credit card usage is governed by Payment Card Industry (PCI) Data Security Standards (DSS). Non compliance with the PCI DSS standards can result in monthly fines to the University of $25,000 or loss of merchant privileges. The sending of unencrypted credit card information (full credit card numbers, security codes, etc.) via email violates PCI DSS 1.1 requirement 4.2.

Why might you care to be stingy in giving out your Social Security Number (SSN)?

General ID Theft Statistic Highlights:

- According to the U.S. Department of Justice Statistics, identity theft is now passing up drug trafficking as the number one crime in the nation.
- According to a 2006 Gartner study victim population was at 15 million victims.

2004 Identity Theft Resource Center (ITRC) study Highlights:

- 18% said that it took them four years or more to discover that their identities had been misused
- It took between 3 hours to 5,840 to restore an identity. This difference is due to the severity of the crime- a lost credit card vs. the use of your Social Security number.

- Even after the thief stops using the information, victims struggle with the impact of identity theft. That might include increased insurance or credit card fees, inability to find a job, higher interest rates and battling collection agencies and issuers who refuse to clear records despite substantiating evidence of the crime. This may continue for more than 10 years after the crime was first discovered.

2004 Bureau of Justice Statistics Highlights:

- Most common age was between 18-24, those in urban or suburban areas, and those in the highest income bracket ($75,000 or more) were the most likely to experience identity theft.
- 3 in 10 households experiencing any type of identity theft discovered it by missing money or noticing unfamiliar charges on an account; almost 1 in 4 were contacted about late or unpaid bills.
- About 1 in 6 victimized households had to pay higher interest rates as the result of identity theft, and 1 in 9 households were denied phone or utility service. Households were equally likely to be turned down for insurance or pay higher rates, be the subject of a civil suit or judgment, or be the subject of a criminal investigation.

I'll need your SSN to process your burger request!

A SSN is often requested regardless of need (many times making it appear like service will not be rendered without it). Additionally, people freely give out their SSN (at times without being prompted). It is difficult to distinguish legitimate requests or need from those that are not.

There are certain times when SSNs should be used. This is not a complete list, but here are some of the situations when they are needed:

- Most financial transactions
- Employment records
- Tax returns (federal and state)
- Medicare benefits
- Contact with the Social Security Administration
- Used by the military & state police to identify its members
- Applications for a hunting, fishing or other recreational license.

The Privacy Act of 1974, which is the primary law affecting the use of SSNs, directs agencies which request a SSN (verbally or on a form) to inform individuals of three things:

1. Whether the disclosure is mandatory or voluntary,
2. By what statutory or other authority the SSN is solicited, and
3. What uses will be made of the number.

Are there other types of sensitive data?

The Office of the CTSO recommends the use of a Sensitive Data chart by the university community (especially data owners, data custodians, application developers & database administrators) as a mechanism to evaluate risks associated with information assets and in formulating appropriate controls.

From this chart you will observe that credit card information and SSNs fall into the highest risk area for both financial & personal fraud. Other highly sensitive data includes things like Student Records, Personal Healthcare Information and PINSs or passwords. You may observe that "names" fall into the second highest risk level. That is because what may make data more sensitive is combining it with data that makes it personally identifiable.

So what should we do or not do?

- There is nothing wrong with using sensitive data to conduct business as long as we educate each other on its proper use, protect it during its useful business life, retain it only as long as required and dispose of it properly.

- Evaluate your business processes for the need to take in or store sensitive data and if indeed it is needed ensure that appropriate protection (obfuscation, masking, one-way hash, encryption, etc.) is applied throughout the data life cycle (PCI DSS 1.1 Requirement 3.1 & 3.4).

- Excessive retention of sensitive data beyond that needed for business purposes or required by law extends the risk to sensitive data unnecessarily. Based on guidance from the state of Illinois retention of credit card data is 3 years. Older credit card data should be deleted (if in electronic form) or shredded (if in paper form).

- Ensure that obsolete computers and electronic media (anything that can store data such as CDs, DVD, thumb drives, diskettes, iPods, etc.) are disposed of properly to ensure that no data remenits remains. This may entail physical destruction of the computer's hard drive (or electronic media) or may instead entail electronic measures such as Department of Defense (DOD) approved erasing of the hard drive. University Technology (uTech) has procedures and technologies in place to dispose properly of university computers. Check with your college technology representative or University Technology (uTech) for details.

- Obfuscation or the masking of a significant portion of the sensitive data (all but the last 4 digits of a credit card number) is a good method to reduce the risk associated with sensitive data on paper such as paper forms, receipts, etc. For data that no longer has business value obfuscation reduces the risk associated with keeping obsolete business records for the remainder of their retention period.

- Certain communications channels such as email, wireless, IM, chat, FTP & telnet are poor choices for the sending or receiving of sensitive data. The data (and possibly authentication information) travels in clear text providing no protection.

- Ensure that business processes do not allow for the sending of unencrypted credit card data via email (PCI DSS 1.1 Requirement 4.2). If you must send sensitive data via a non secure channel

such as email, consider using encryption built-in to common office productivity applications such as newer versions of Microsoft Word, Excel, PowerPoint, Adobe Acrobat, Winzip, etc.

- Credit card information must not travel over non-secure wireless networks (PCI DSS 1.1 Requirement 4.1.1). University Technology (uTech) is in the process of instituting secure wireless across the university. Check with your college technology representative, uTech or the business office for guidance on compliance with this requirement.
- The security code on the back of a credit card must not be stored in electronic or paper form after obtaining authorization (PCI DSS 1.1 Requirement 3.2.2).

In a world that retains so much data, with or without our knowledge, it may be prudent to reflect before transmitting or storing data unnecessarily. Let's not regret tomorrow what we transmit or retain today.

Best Regards,

Michael Rodriguez
CTSO @ Western Illinois University
ma-rodriguez2@wiu.edu

"*If you reveal your secrets to the wind, you should not blame the wind for revealing them to the trees*. "— Kahlil Gibran