



April 2009

We've updated The Compass to compliment our new website design!

See what else is new by **visiting us** on the web.

Meet Experts of The Compass at the Following Events:

2009 Calendar of Events

05|03 PCBB Executive Management Conference, San Francisco, CA

05|13 TBA Annual Convention & Exposition, San Antonio, TX

05|31 WIB Annual CFO, Investments & Operational Risk Conference, San Francisco, CA

Archive Download

Download a printable PDF to share with colleagues or access **The Compass** archives:

» The Compass, April 2009 - **Download** (PDF)

» The Compass - **Archives**

Sign up to receive The Compass monthly.

Not already on our mailing list? Our monthly newsletter will help you keep abreast of industry and regulatory developments for the financial industry. **Sign up now!**

Contact us!

We are constantly working to improve **The Compass** and appreciate your feedback! Send your comments to: **education@compushare.com**

Rate this article!

Click here. Your response will take less than 1 minute!

Your Biggest Security Threat May Already Be On Your Network

by **Jeff Porn**
Information Security Consultant
Compushare, Inc.

With technology now reaching into nearly every aspect of your business, keeping your bank or credit union secure has become one of, if not the, biggest challenges IT administrators face every day. The last thing a financial institution wants to worry about is what their trusted employees are doing on the network. Yet, this concern is prevailing as the biggest threat to the security of any company's infrastructure today.

By now, every player within the financial services industry has learned of the data breach that took place within New Jersey-based credit card payment processor, Heartland Payment Systems, in 2008. The event affected more than 625 banking institutions and has been noted as the largest data breach in U.S. history. Although the means by which computer hackers gained access to the accounts has not been disclosed, it is known that the external security measures used to protect Heartland's network were PCI certified. This means that proper firewall practices were being followed. Furthermore, due to the multiple layers of anti-virus and malware protections in place, the company stated that they do not believe the breach occurred by an employee opening an email attachment. So, a potential scenario that I'm sure is being investigated is the possible involvement of an employee with access to the network either through malicious intent or compromised through social engineering. Even with the proper security practices in place, PCI standard certifications and strong encryption, a single compromised employee with access to sensitive data can bypass all of these security measures. In the case of Heartland Payment Systems, key loggers were used on the workstations capturing sensitive data before any encryption was used targeting the weakest point in any security model - the human element.

The main focus of most financial institutions when it comes to security is to protect against attacks from the outside by ensuring that firewalls are in place, configurations are correct, and testing is conducted on a regular basis per Federal requirements. In addition, Intrusion Detection solutions are available that will monitor network traffic for attacks and automatically shut them down, or alert key personnel that a potential attack is underway. Internally, most follow standard best practices for security recommended by Microsoft, Novell, or other recommendations and requirements for the financial industry. However, those practices are ineffective in instances of employees performing unauthorized activities or accessing unauthorized data on the network.

The Identity Theft Resource Center (ITRC) reported that data breaches rose 50% in 2008. Of the many methods used, including insider theft, Malware attacks and hacking, insider theft saw the largest increase of more than double the number from 2007. Data on the move and accidental exposure, both human error categories, account for 35.2% of those breaches that indicate cause. Of the various industries reviewed, the financial industry showed the largest increase in breaches, almost doubling the number of incidents from 2007. In looking at the protections that were in place when breaches occurred, it was discovered that only 11% had either encryption or password protection in place. The bulk of the data that was breached had no protection at all. Here at Compushare, we also saw an alarming 50% increase in the number of clients that were successfully "breached" through Social Engineering testing. The methods used were a combination of email phishing, phone calls and physical site assessments. When at least two of these methods were combined, we saw nearly a 100% success rate in breaching the client or gaining sensitive information.

As technology evolves and becomes more intelligent, hackers have to continually find new security gaps and better ways to circumvent these new levels of security. However, the one thing they can continue to rely on is the fact that there is no patch for human error. This has been, and will always be, the weakest link and the most frustrating security concern that IT administrators face. So what can be done to help mitigate the

threat of employees being targeted or exploited to gain access to sensitive data?

There are two main areas of focus - *Technology* and *Risk and Compliance*. From a technology standpoint, the institution should ensure that the recommended security best practices, controlling who has access to what data and when, are implemented and enforced both at a technological and policy level. All activity on the network should be logged with alert points implemented notifying personnel of any unauthorized activity.

When it comes to Risk and Compliance, there are several areas of vital importance that must be addressed by every financial institution. A Risk Assessment should be performed to determine what your risks are, how to control these risks, and the right measures to take to protect sensitive data across all areas of the network and on the move. Ongoing training must be conducted for all employees on what is considered sensitive data, who should have access to this data, and what to do in a situation where someone asks for, or tries to gain access to, data either through email, phone calls or physical site visits. Testing should be conducted on at least an annual basis to ensure that all the technology, policies and training you have implemented are being enforced and followed throughout your institution. Quarterly testing is required for certain security parameters, such as firewalls.

Technology has evolved to become a required element in business and performing our job functions. Technology is deeply entrenched in everything we do and the protection of sensitive information had become complex and more difficult than ever. However, this does not mean that we throw our hands up and give in to the hackers and attackers. With proper implementation of security best practices, upkeep of policies and procedures, and ongoing training and testing, we stay a step ahead and ensure that our data is protected, access is limited, safeguards are implemented, and employees are informed, aware and ready to act when malicious activity is suspected.

###

Compushare delivers viable and proven solutions exclusively for community financial institutions including areas of information security, risk management, social engineering, business continuity, business resumption, data assurance, compliant messaging solutions and vulnerability management. Learn more about our approach toward **Strategy**, **Safety**, **Soundness** and **Support**.

To learn more on how Compushare can assist your institution through an Information Security Assurance Program or Social Engineering testing and training, contact your Client Solutions Executive or **education@compushare.com**.