case study

Credit Card Heist at the Heartbreak Cafe

By Galen Collins

Introduction

Owner Tom Petrov experiences a payment-card breach at one of his restaurants, the Heartbreak Café. The case study scenario provides the details of the security breach and the subsequent forensics investigation. Payment Card Industry (PCI) compliance and security issues are addressed. It concludes with several questions about payment card security and the appropriate remedial responses to the incident. The purpose of this case study is for readers to gain a solid understanding of the importance as well as the basic components of payment card and network security. Point-of-sale (POS) systems continue to be the easiest way for criminals to obtain the data necessary to commit payment-card fraud (Trustwave, 2011).

Background Information

The Heartbreak Café, a franchise and an upscale fast-casual restaurant, is located in a US international airport. The franchise company, through slow and careful growth as well as expanded menu offerings, has established a strong brand and reputation. It provides extensive pre-opening assistance in site selection and preparations (e.g., layout, furniture, fixtures and equipment), training (e.g., policies and procedures, food preparation and customer service), and operational support (e.g., guides and forms for day-to-day operations and point-of-sale system advice).

Tom Petrov, a Russian immigrant, owns and manages the Heartbreak Café. Tom, young and penniless during the last days of the Soviet Union, received a plane ticket to America from a wealthy classmate. With little money and poor in English, he became a dishwasher at a Chinese restaurant. Loving the restaurant business, he enrolled in a top-ranked hospitality school and worked his way through college by waiting and bussing tables. He later cooked and eventually managed a small deli. In 2002, after successfully managing several full-service, independent restaurants, he decided to become an entrepreneur and opened up his first restaurant. He now owns and operates four restaurants featuring simple well-made food. Tom says, "It's meant to be fun and taste good – it doesn't have to be fancy."

The Heartbreak Café has been profitable since its inception in 2007. Every year, customer counts and sales have grown. Tom attributes its success to providing customers with excellent customer service and good-quality, affordable food. The café serves breakfast, lunch, and dinner daily from 6:00 AM until 10:00 PM. Limited seating is provided near the café. More than half of the customers take prepared items to eat on the airplanes. Approximately 20 percent of the customers are airport employees.

Galen Collins *is affiliated with Northern Arizona University.*

The Restaurant Network

As in a cafeteria, customers take trays, order menu items from an order board, and pay the cashier. A restaurant POS system, Restron, is used for processing payments. It enables customers to pay with credit or debit cards. The cashier swipes the customer's card into the POS payment system, which uses an application for processing the payment over an Internet connection. Card transactions are sent electronically via a payment processing company, PayTech, to an acquiring bank for authorization, capture, and deposit for payment.

In May, 2011, the POS system consisted of three POS terminals connected to a server in the back office. The server, a storage device, contained information generated by the POS and card processing software, generic business applications (e.g., Microsoft Office), and digital video recording (DVR) software for the surveillance cameras monitoring the POS workstation and back office areas.

The server and the surveillance camera system were connected to the Internet via a residential cable modem router. The network had an inadequate firewall, a technological barrier for guarding against inbound and outbound Internet threats, such as hackers and malware or any software (e.g., viruses, worms, Trojan horses, spyware, etc.) designed to exploit a computer without consent. The only other protection was outdated antivirus software.

The POS system was purchased from a Restron reseller, RPA, which also provided hardware and software support. In 2009, the Restron reseller network dropped RPA because of financial problems but Tom continued to use RPA as they provided support that kept the POS system functioning smoothly. This arrangement, however, precluded the updating of the POS system software. Consequently, the version of the POS payment application was not compliant with Payment Application Data Security Standard (PA-DSS). For example, stored magnetic card track data was not kept unreadable (e.g., encrypted). Furthermore, the debit card personal identification number (PIN) device, which encrypts customer PIN numbers at the point of sale through to

the bank for verification and payment, was also not in compliance with PIN Transaction Security (PTS) requirements. In 2010, Visa mandated an update of the PTS to a triple data encryption standard (TDES), a stronger, more robust encryption standard to keep pace with the encryption cracking services and decoding ability of tech-savvy criminals draining bank accounts.

PA-DSS and PTS are part of the overall Payment Card Industry Data Security Standard (PCI-DSS). PCI-DSS contains a set of regulations or rules developed jointly by the leading card companies (e.g., American Express, Visa, MasterCard, etc.) to prevent cardholder data theft and to combat credit card fraud. The key requirements of PCI-DSS are (https://www.pcisecuritystandards.org):

- **Build and Maintain a Secure Network**
  - Install and maintain a firewall configuration to protect cardholder data.
  - Do not use vendor-supplied defaults for system passwords and other security parameters.
- **Protect Cardholder Data**
  - Protect stored cardholder data.
  - Encrypt transmission of cardholder data across open, public networks.
- **Maintain a Vulnerability Management Program**
  - Use and regularly update antivirus software.
  - Develop and maintain secure systems and applications.
- **Implement Strong Access Control Measures**
  - Restrict access to cardholder data by business need-to-know.
  - Assign a unique ID to each person with computer access.
  - Restrict physical access to cardholder data.
- **Regularly Monitor and Test Networks**
  - Track and monitor all access to network resources and cardholder data.
  - Regularly test security systems and processes.
- **Maintain an Information Security Policy**
  - A strong security policy sets the security tone for the whole organization and informs employees and vendors what is expected of them.

In 2009, Restron had their payment application certified as PA-DSS compliant by a Qualified Payment Application Security Company. Software by definition cannot be PCI-DSS compliant. PCI-DSS compliance entails other facets such as the network configuration and system policies and practices.

Using an RPA communication program, Tom frequently accessed the restaurant POS and surveillance systems via the Internet remotely. This software was also used by RPA for providing remote technical support. Tom and RPA support personnel gained access with the same user ID and password which never changed.

Credit Card Heist

On July 5th, 2011, Jill Sanchez, a Heartbreak Café cashier, overheard customers discussing a police report they had filed. All of them who had worked together in the same airport department had credit or debit card information stolen recently. She told Tom. Tom also had discovered a fraudulent charge on his credit card.

The next day, Jim Brown, a local police detective that Tom knew and worked at the airport, asked him what was going on with his credit cards. Tom replied: "What do you mean?" Jim responded, "The credit and debit cards of at least 10 airport employees and maybe more have been fraudulently used. We are looking at common places the victims ate and your restaurant is at the top of the list." "I'm not worried," said Tom. "I'm 110% percent sure that our system has not been compromised." Jim advised him to immediately check the restaurant network for security breaches. "I have contacted the U.S. Secret Service," stated Jim. "But why?" asked Tom nervously. "Because they have primary jurisdiction over credit card crimes," replied Jim."

Tom checked with RPA and the payment processing company for any incriminating evidence. RPA performed a server scan that did not detect crimeware, a class of malware to automate cybercrimes. The payment processing company noticed no fraudulent card activity associated with their customers. Consequently, the credit card companies had not initiated forensic investigations. Still concerned, Tom recalled his own credit card incurring a fraudulent charge at the café.

The next day Tom met with the RPA, the police department, and the U.S. Secret service. "I am glad that all of you could attend this meeting to help determine if the Heartbreak Café has a problem. The server scan revealed nothing," stated Tom. The U.S. Secret service representative, April Clark, looked at the server scan. "This scan readout is not for this restaurant," stated April. Evan Thompson, the RPA representative, looking chagrined, apologized for the mistake, "We inadvertently scanned the wrong location." Tom was crestfallen. His feelings were confirmed when the second scan detected crimeware. He immediately shut down the Heartbreak Café network.

"I assumed the system was secure and customer account data safe," stated Tom. "You are not alone, Tom," replied April, with an empathetic look on her face. She continued, "Restaurants regained its title as the most breached industry -- representing 57% of the investigations according to the 2011 Global Security Report authored by Trustwave (2011), a provider of on-demand data security and payment card industry compliance management solutions. Many restaurateurs do not understand the magnitude of this problem and lack the technological sophistication of larger companies. Restaurants are frequently targeted by organized thieves because of the high volume of card transactions and the low level of security in place. The threats of theft are increasing as sophisticated techniques to hack into systems

evolve. Staying on top of the latest fraud trends is key to minimizing losses and maximizing cardholder protection. In 2010, the average cost of a breach was $214 per compromised record according to the Ponemon Institute (2011), a privacy and information management research firm. Do the math Tom. A breach involving 500 customers could cost you more than $100,000 in damages."

"Are you aware of PCI-DSS compliance requirements?" inquired April. Tom responded, "Not really. I never received any information or training about them from the franchise company or my payment processing company and POS reseller. I feel like I have been left in the dark, until now. This incident has also been a wake-up call for the Heartbreak Café franchise company executives. They now realize that the brand and reputation of the company could be harmed because of substandard corporate governance. "Tom, it is interesting to note that many companies now mitigate risks by mandating franchisees and suppliers to have certain levels of security in place before they will transact with them (Knights, 2011). What is the next step?", asked Tom. "We will conduct a full-blown forensic investigation," replied April.

The breach was recognized early fortunately so no action was taken by the credit card companies or acquiring bank for non-PCI-DSS compliance. As a result, Tom did not have to pay card damages, hire a PCI-DSS qualified incident response assessor (e.g., Trustwave) for determining how unauthorized parties had obtained card data, or pay a fine. Fines can be in the $5,000 to $50,000 range and the cost of an assessor can be up to $25,000 (http://www.restaurantdatasecurity.com/faqs.htm). It takes one card breach to potentially put a restaurant out of business. Tom was lucky and grateful.

Forensics Investigation

The Secret Service investigation entailed the following:

Interviewing employees. All of the employees, including Tom, were interviewed and their records were evaluated. Tom's connections in Russia were questioned, which made him feel a bit uncomfortable. April explained that crime groups from Russia and the former Soviet states are among the largest purveyors of credit card fraud in the US. One employee's profile fit that of a potential card thief but the investigation exonerated him.

Inspecting the crime scene. April looked for skimmers, reviewed surveillance videos to spot unusual employee behavior, and took fingerprints on the server workstation. "What are skimmers?," inquired Tom. April replied: "They are card-swipe devices used to steal card data. Handheld skimmers are often used in restaurants. Some are about the size of a cigarette lighter and are easily concealed. Skimming devices are available online for as little as $300. Last year, I investigated a case where a 20-year-old server was paid $10-$15 for every card he skimmed. Skimmers can also be attached to the POS terminals. The fraudster returns after a period of time to replace the device, collecting the stolen card data." "What else have you looked for?" asked Tom. April answered, "Video evidence of someone downloading crimeware from a flash drive or from the Internet to the server." The crime scene revealed nothing.

Examining the digital evidence. The Secret Service confiscated the server. The digital evidence was extracted and analyzed in a forensic laboratory. The RPA scan finding of crimeware was confirmed.

"April, what is crimeware exactly?" inquired Tom. "It is like evidence found after a robbery like a crowbar used to open a door, " replied April. She went on, "The intruders were able to remotely access the POS system via the Internet and steal card data. Organized crime groups are suspected of obtaining the stolen card numbers through dump sites on the Internet - most likely from out of the country." "What did they do with the card data?" asked Tom. April replied, "Credit cards with new names were manufactured. The cards were used for purchasing gift cards at retails places, such as Target, and then sold on the street in various US cities at discounted prices."

What is the Remediation Plan?

Tom had to get the Heartbreak Café network back up and running quickly. Significant changes, however, were required to make it secure and PCI compliant. He contacted Michael Higgens for help. Michael was an account representative with FBPS, the current Restron reseller. Michael informed Tom that the Restron POS system was PA-DSS compliant. "Can you help me with the other PCI-DSS requirements?" asked Tom. Michael responded, "Yes, we offer a bundle of products and services that strengthen security instead of just meeting compliance standards. Keeping on top of this is tough though. Compliance requirements are ever changing and complicated." "I know," replied Tom. "I just received a 30-page PCI- DSS Self Assessment Questionnaire (SAQ D). What is the SAQ D?" Michael answered, "An annual report submitted to your acquiring bank confirming PCI-DSS compliance. "Who can help me with this?" asked Tom. "You can hire a qualified security assessor, an approved PCI security and auditing firm. Also required is proof of a quarterly external network scan through a PCI-DSS approved scanning vendor," replied Michael. "Does passing the external scan mean that the location has no security risks?" asked Tom. "No,"replied Michael. He continued, "It means that it is not vulnerable to some of the common methods hackers use from the Internet to illegally enter a network without permission." "How about internal vulnerability scans?" inquired Tom. Michael responded, "Our security services will constantly check for threats and issues on the local area network that could be exploited to reveal cardholder data. While the card brands do not require the submission of internal scan results for validation purposes, merchants must demonstrate they are working to resolve any issues discovered by internal scans."

"How vulnerable are restaurants to credit card heists?", inquired

Tom. "Very vulnerable if they do not have the right technology and processes in place," replied Michael. " Furthermore, a recent study of fraud prevention strategies practiced at small to mid-sized businesses conducted by the National Retail Federation and First Data Corporation revealed that 60% of the respondents are unaware of the possible consequences of a breach, such as a significant financial setback, bankruptcy, severely damaging negative publicity, high customer attrition, and termination of business relationships (First Data Corporation and National Retail Federation, 2011; Epstein and Brown, 2008). Two-thirds believe that their business is not vulnerable to cardholder data theft. There are many security risk points, including (Slawsky 2011):

- POS terminals and PIN entry devices.
- Employees.
- Third party vendors.
- Servers for processing and storing cardholder data.
- Payment applications.
- Routers and other network devices.
- Internal and external (Internet) networks used for cardholder data.
- Physical security of the building and devices used for cardholder data.
- Internal card processing procedures and access controls.
- Procedures for monitoring security and responding to vulnerabilities.
- Portable devices (e.g., USB flash drives, skimmers) that could link to cardholder data."

"I have so much to learn," sighed Tom. Michael responded, "Many restaurants and other small businesses are prone to costly security breaches because of a gap in merchant-security education (Guisti 2009; 2011). The Heartbreak Café incident is all about risk management, protecting your customer information and business from being vulnerable. It entails the identification, measurement, and control of uncertain events to minimize loss and optimize the return on the money invested for security purposes (Finne, 2000). Every phase of customer information (creation, transfer, storage, viewing, and destruction) must be considered as it is used by the organization and its partners. We will need to implement the appropriate risk-control strategies and solutions for application security (e.g., POS payment software), infrastructure security (e.g., hardware and networks), operational security (e.g., procedures and processes), organizational security (e.g., employee and contractor background checks and training and awareness programs), compliance (e.g., PCI), third-party security management (e.g., new security risks introduced), and business continuity planning (e.g., monitoring and testing security measures and incident response) (Kapuria, 2005). "

Discussion Questions

1. Why should payment card security be an important issue to Tom?
2. Why was payment card security not a priority at the Heartbreak Café?
3. How should Tom view and approach PCI-DSS compliance?
4. What should be the roles of the franchisee, the franchisor, and the payment processor in PCI-DSS compliance?
5. What key actions would help prevent the type of security breach experienced at the Heartbreak Café and make the network secure?

Glossary of Acronyms and Terms

- DVR - Digital Video Recording
- FBPS - Name of current Restron point-of-sale reseller
- PA-DSS - Payment Application Data Security Standard
- PayTech - A payment processing company
- PCI - Payment Card Industry
- PCI-DSS - Payment Card Industry Data Security Standard
- PIN - Personal Identification Number
- POS - Point-of-Sale System
- PTS - PIN Transaction Security
- Restron - Name of point-of-sale system used
- RPA - Name of old Restron point-of-sale reseller
- SAQ D - PCI-DSS Self Assessment Questionnaire
- TDES -Triple Data Encryption Standard

References

Ataya, G. (2010). PCI DSS audit and compliance. *Information Security Technical Report*,15(4), 138-144.

Berezina, K. (2010). Top issues in PCI DSS compliance in hotels: an exploratory study. *Journal of Hospitality and Tourism Technology*, 1(2), 218 – 233

Edmonds, J. (2011). Managing successful change. *Industrial and Commercial Training*, 43(6), 349-353.

Epstein, R. A. & Brown, T.P. (2008). Cybersecurity in the payment card industry. *The University of Chicago Law Review*, 75 (01), 203-223.

Finne, T. (2000). Information systems risk management: Key concepts and business processes. *Computers and Security*, 19(2), 234-242.

First Data Corporation and National Retail Federation (2011). Small Merchant Data Security Survey Results. Atlanta, GA: Authors.

Hosak, b. (2011). Business still unaware of the risks of account data compromise. Computer Fraud and Security, 2011, (1), 17-19.

Guisti, A. (2009). PCI compliance made easy for restaurants accepting credit cards. QSRweb.com. Retrieved 10th of January 2012 from http://www.qsrweb.com/whitepapers/2319/PCI-Compliance-Made-Easy-for-Restaurants-Accepting-Credit- Cards.

Guisti, A. (2011). ISO's can teach merchants to look for security threats, even from the inside. ISO & Agent, 23-28.

Kalkan, K., Kwansa, F., and Cobanoglu, C. (2008). Payment card industry data security standards (PCI DSS) compliance in restaurants. *Journal of Hospitality Financial Management*, 16(2), Article 3.

Kapuria, S. (2005). Steps for managing risk. Computerworld. Retrieved 11th of June 2012 from http://www.computerworld.com/s/article/106101/Steps_for_managing_risk?taxonomyId=17&pageNumber=2.

Knights, M. (2011). IT security legislation guide. *Engineering and Technology,* 6(7), 63-65.

Ponemon Institute. (2011). 2010 U.S. Cost of a Data Breach. Traverse City, MI: Author.

Rees, J. (2010). Information security for small and medium-sized business. *Computer Fraud and Security*, 2010(9),18-19.

Slawsky, R. (2011). Frequently Asked Questions about PCI Compliance. Reston, VA: NetWorld Alliance.

Tutton, J. (2010). Incident response and compliance: A case study. *Information Security Technical Report*, 15(4), 145-149.

Trustwave. (2006). Protecting Cardholder Data for Hospitality Businesses Accepting Payment Cards through Multiple Channels: Hotels, Motels and Lodging. Chicago, IL: Author.

Trustwave (2010). Hospitality Breaches on the Rise. Chicago, IL: Author.

Trustwave (2011). Global Security Report 2011. Chicago, IL: Author.

Vaca, J. (2010). Network and System Security. Burlington. MA: Elsevier.

Vellayan, N. (2011). PCI compliance: What your franchise should know International Franchise Association. Retrieved 4th of January 2012 from http://www.franchise.org/Franchise-Industry-News-Detail.aspx?id=55439.