Brief Case Summary and Importance of Topic

Hackers gained access to the Heartbreak Café restaurant network by guessing or "cracking" the RPA communication program (remote desktop software) passwords or by using malware to penetrate the firewall. Once in, they downloaded logging software to harvest card data from disk or volatile (e.g., RAM) storage or as it traversed the network. They also downloaded crimeware for creating a backdoor (bypassing normal authentication for future access) and posting the card data collected from the logging software onto Internet dump sites where it was accessed by criminals for manufacturing counterfeit credit cards. The Heartbreak Café was unprepared to deal with payment-card breach. The restaurant network was insecure and not PCI-DSS compliant. Guisti (2009; 2011) maintains that many restaurants and other small businesses are prone to costly security breaches because of a gap in merchant-security education. The key goal of this case study scenario is for students to gain a solid understanding of the importance as well as the basic components of payment card and network security.

Target Audience

This case would be appropriate for an undergraduate or graduate information technology or capstone course.

Teaching Objectives

- Learn about PCI-DSS and the key requirements (information presented in the case study and in the introductory lecture on the case study topic).
- Understand both the flow of transaction data through the various components that comprise the payment card industry and the relationships between the various organizations involved in PCI-DSS compliance (information presented in the case study and in the introductory lecture on the case study topic).
- Understand the consequences of payment-card breaches and the circumstances resulting in network security vulnerabilities (information presented in the case study and introductory lecture on the topic, Question 1 and 2 answers).
- Identify the roles and responsibilities involved in network security and PCI-DSS compliance (question 3 and 4 answers).
- Identify both key network security risk points and the appropriate remedial actions required (information presented in case study, question 5 answer).

Teaching Approach

This case uses a problem-solving approach where students identify issues within the case study and respond to the solution-focused questions at the end of the case.

Step 1: Class lecture that introduces the case study topic.

- Show students the video: PCI Compliance - RSPA Project: PCI (http://www.youtube.com/watch?v=7W-k3R2N7Zk). This video shows a candid, inside look at the facts surrounding PCI Compliance and reveals how costly compromises can be to a restaurant.
- Show students the site: Restaurant Data Security (http://www.restaurantdatasecurity.com). This site provides a video and information on restaurant security services provided by Radiant Systems, a provider of POS technology to the hospitality and retail industries.
- Have students read the article: Gallagher, S. (2011). How hackers gave Subway a $3 million lesson in POS security: Retrieved 2012-01-10, from http://arstechnica.com/business/news/2011/12/how-hackers-gave-subway-a-30-million-lesson-in-point-of-sale-security.ars.
- Additional materials for helping the instructor prepare for the class lecture and case study discussion:
    1. Arceneaux, P., (2011). Under lock and key: PCI compliance and data security is sound business practice. Retrieved 2012-01-17, from http://www.franchising.com/articles/under_lock_and_key_pci_compliance_and_data_security_is_sound_business_pract.html..
    2. Thakar, S. and Ramos, T. (2009). PCI for Dummies. Retrieved 2012-01-15, from http://static.progressivemediagroup.com/Uploads/Whitepaper/241/1321e0c1-a09b-4ebc-b4de-5e3427f9ab46.pdf.

Step 2: Homework assignment. Students read the case study carefully, highlighting main points, organizing relevant events chronologically, and noting consequences of actions taken.

Step 3: In class or as a homework assignment, students perform a case analysis, individually or in a group. Issues requiring attention are identified and ordered according to importance, from major to minor. They then answer discussion questions based on their case study findings.

Step 4: The instructor starts and facilitates a class discussion on the case study by asking someone (or a group) for an answer to a particular discussion question and then works backwards to derive the analysis. For example, the instructor could ask a student to identify a specific action that would help prevent a security breach at the Heartbreak Café. The student could suggest stronger password security. The instructor would then ask the student to identify existing password security weaknesses (e.g., password never changed, every user had the same user ID and

password). The instructor then would ask the student to describe specific solutions (e.g., unique user IDs and passwords; two-factor authentication).

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

Answers to Discussion Questions

1. Why should payment card security be an important issue to Tom? When a restaurant implements and maintains a strong security posture, it is taking an aggressive stance on protecting customer information. But most importantly, a secure organization will not spend time and money identifying and responding to breaches that could jeopardize its viability (Vaca, 2010). Tom was fortunate. Because of the chatter among customers who worked at the airport, the payment-card breach was detected early and Tom quickly intervened in a responsible manner, minimizing the cost of the data breach and negative publicity. Most small businesses suffering from payment-card breaches, however, often incur costs that far outweigh those costs associated with taking a proactive approach to eliminating the risk by becoming PCI-DSS compliant (Kalkan Kwansa, and Cobanoglu, 2008; Hosack, 2011). POS systems continue to be the easiest way for criminals to obtain the data necessary to commit payment-card fraud (Trustwave, 2011).

2. Why was payment card security not a priority at the Heartbreak Café?

   Tom did not fully understand or underestimated the *risks* and consequences associated with a *payment-card breach*. A lack of awareness among restaurateurs about payment card security has made restaurants a prime target of identity thieves (Guisti, 2009).

   Restaurant operators, like Tom, often rely on the POS resellers or vendors to be their de facto IT department. It is important to remember that the POS system is just one component (PA-DSS) of the overall PCI- DSS requirements. POS resellers may not address PCI-DSS compliance or offer comprehensive solutions (e.g., Houston-based Vendor Safe Technologies) that ensure secure restaurant networks and PCI-DSS compliance (Berezina, 2010; Trustwave, 2011)

   Everyone likes a comfort zone. Tom continued to use older system technology because the vendor, Restron, kept the POS system functioning smoothly. Edmonds (2011) maintains that fear is a common reason for resisting change - fear of the unknown, of failure, loss or leaving a comfort zone.

   Tom's main focus, like other restaurant operators, was on selling quality food rather than computer security.

   Tom may have thought his business too small to be the target of hackers or malware, which according to Rees (2010) is a widespread belief among small businesses.

3. How should Tom view and approach PCI-DSS compliance? PCI-DSS should be viewed as a means for making the restaurant system secure and protecting cardholder data and not as a checklist that must be filled out to meet compliance requirements (Slawsky, 2011). Parts of it are difficult to understand and implement (Berezina, 2010; Slawsky, 2011). Expert assistance is needed to identify appropriate tools and services to achieve compliance.

4. What should be the roles of the franchisee, the franchisor, and the payment processor in PCI-DSS compliance? PCI-DSS standards put the responsibility for payment data security back on restaurant owners or franchisees. They are ultimately accountable for firewall protection of data, system IDs and passwords, antivirus software, restriction of access to data, and network security, etc. Tom, however, had not received any guidance about PCI-DSS compliance from the franchisor or the payment processing company. Most franchisees lack security expertise and cite PCI-DSS as too costly and difficult to maintain according to Nina Vellayan (2011), the CEO and president of Frontstream Payments, a provider of merchant account and payment processing services. Vellayan (2011) recommends that franchisors adopt a three-pronged approach to help franchisees comply with

PCI- DSS and to secure cardholder data:

- The franchisee contracts should include a data security policy consistent with the PCI-DSS to drive compliance.
- Implement regular training and education programs to teach franchisees the fundamentals of data security. Include methods for cardholder data security practices in the standard operating procedures.
- Partner with a payment processor with a professional staff and educational materials to assist with both the understanding and the implementation of PCI-DSS requirements. A good processor provides frequent updates and assistance when requirements change.

5. What key actions would help prevent the type of security breach experienced at the Heartbreak Café and make the network secure? Key actions that Tom needs to take are (Trustwave, 2006;Trustwave, 2010; Ataya, 2010; Tutton, 010; Trustwave 2011):

Issue 1- Infrastructure and Operational Security: Poorly configured router/firewall and network. Action: Use two servers, rather than one, and a commercial-grade router/firewall that enables the POS system (POS and card data on server and zone 1) and the general network (email, business applications and DVR software on server and zone 2) to be located in separate security zones, each with its own security policies. This will enable strict control and management of user access, blocking threats (e.g., malware and hackers) and unauthorized data transmissions to the Internet. This will also prevent unnecessary communication to the cardholder environment, which should not be directly accessible via the Internet (all inbound traffic blocked), and ensure that users only have access to files and data that they are permitted.

Issue 2 - Application Security and Operational Security: Outdated antivirus software. Action: While the firewall is programmed to block malware, it may be compromised. The next line of defense is antivirus software, which prevents, detects, and removes malware. In order to be an effective defense, however, the antivirus software must be kept updated to recognize new versions of malware and run in the background at all times.

Issue 3 - Application and Operational Security: Weak password scheme. Action: Use two-factor authentication, which provides an additional layer of security when accessing the Heartbreak Café network remotely. The first factor is typically the user ID and password. The second factor is information unknown to the user, such as a random six-digit number or passcode sent to an authorized user's cell phone or email account. The passcode, keyed in below the user ID and password, typically expires within two minutes. Users have unique IDs and passwords, which should be changed on a regular basis.

Issue 4 - Application and Infrastructure Security: Card and PIN data insecure. Action: Use only POS software that is PA-DSS certified and PIN entry devices that are PTS certified. This ensures that card and PIN data will be difficult for hackers to compromise. A promising new solution is tokenization, which is the process of exchanging card data with a token (a unique identifier to cardholder data) at the point of swipe and storing the card data on the payment processing company system. With no card data present , the scope of the PCI-DSS compliance is significantly reduced.

Issue 5 - Organizational and Operational Security, Third-Party Security Management, Business Continuity Planning: Lack of security awareness, knowledge, and plan. Action: Develop a security policy for employees and vendors. Ensure daily procedures meet PCI-DSS requirements. Educate employees on their specific roles and tasks in protecting payment card data. Carefully hire employees to limit security risks. Require vendors that have access to card data to also comply with PCI-DSS. According to the 2011 Global Security Report, 88 percent of data breaches in 2010 resulted from insecure software code or lax security practices in the management of third-party technology. Finally, create a detailed plan for responding to security breaches and monitor and test security measures on a regular basis.