

DSI

DATA SECURITY INVESTIGATIONS

Anatomy of two breach scenarios with two very different outcomes

By Richard H. Gamble

EPISODE ONE

The following account of a data security breach is fictional, but the details describe the way security breaches do occur in the real world. It was written by an anonymous executive officer at a data security firm, and by Richard Gamble.

June 12, 2008, Bangalore, India: Rajiv Chandri rides his bicycle seven miles to the office where he works as a database administrator for an Indian firm that provides outsource services to multinational corporations and checks in with his badge at security checkpoint. He's worried because his wife was recently laid off from her telemarketing job and the auto company has repossessed their car. Using his super-user credentials, he logs in to the CRN database for QualitiMart, a large U.S.-based retailer, to check on the status of daily backups. Then, just for the fun of it, he runs a "SELECT" query on the credit card table. Not surprisingly, the query returns hundreds of thousands of credit card transactions for QualitiMart stores. He logs off quickly and a little guiltily, but he's not really worried because he knows that his actions aren't being monitored.

June 13, 2008, St. Paul, Minnesota: James Watkins, head of data security at QualitiMart logs on and reviews the day's activity shown in his security incident and event management (SIEM) system. He sees nothing unusual in the activity, which shows that Chandri has logged on, something he does five days a week because that's his job as a database



administrator responsible for file backup. Watkins takes comfort in knowing that the SIEM, which QualiMart upgraded last year, is monitoring all activity and that QualiMart's data security got a clean bill of health three months ago in its PCI compliance audit. He knows that the system is not foolproof, that there are millions of database transactions executed every day and tracking all of them—especially SELECT queries—using native database auditing would simply overwhelm the system.

June 14, 2008, Bangalore: Chandri runs the SELECT query again and nervously downloads the first 50 transactions onto his BlackBerry and then logs out.

June 18, 2008, Moultrie, Georgia: Phyllis Morgan goes to QualiMart to buy back-to-school clothes and supplies for her three children, charging \$327.74 to her credit card.

June 22, 2008, Bangalore: Since there have been no repercussions, Chandri downloads 100,000 credit card transactions onto his BlackBerry shortly before his shift ends. He goes to his PC at home and spends hours at Internet chat rooms searching, as "Reliable Provider," for someone who might buy the data. Eventually he gets three promising responses, one of which, "RBL Ventures," offers up to \$20 per card.

June 22, 2008, Bucharest, Romania: Egon Elesciuc gets a fresh cup of coffee and then sits down to watch traffic on an Internet chat room. He sees the message from "Reliable Supplier" and answers that he is interested and would pay up to \$20 for full information about currently valid credit cards.

June 23, 2008, Bangalore: Chandri goes to a local library that has online computers and contacts the e-mail address that offered \$20 and describes

[COVER STORY]

what he has for sale. He has to leave before he gets any response. His wife is upset because their baby is sick, their credit cards are maxed out because the issuer has recently reduced the credit limit, and they have no money for medicine. He logs onto his PC and sends a message to the same address.

June 24, 2008, Bangalore: Chandri receives a message back from “RBL Ventures,” asking him to show them a sample of 100 transactions so they can evaluate the data. Four hours later they e-mail back offering \$12 per usable card. He e-mails half the data. RBL responds an hour later, saying there’s usable data on 42,174 valid, separate cards. They offer to pay him \$506,088 for those cards and will wire the funds to his bank account. He e-mails his bank account information.

June 24, 2008, Bucharest: Elesciue gets the first 50,000 credit card transactions from “Reliable Supplier” and runs the numbers through a program that spots duplicates and weeds out cards known to have expired or been cancelled. He subtracts another 2,000 for good measure and offers \$12 to a seller he thinks is inexperienced.

June 25, 2008, Bangalore: Having confirmed that the funds are in his bank account, Chandri sends the other 500,000 transactions and gets a wire transfer for \$464,088 for 38,674 cards.

June 28, 2008, Bucharest: Elesciue takes the credit card data to an associate who manufactures counterfeit credit cards.

July 12, 2008, Bangalore: Chandri buys a new car for cash, then takes his family shopping. He invests the money in bank CDs.

July 14, 2008, Bucharest: Elesciue distributes the counterfeit cards to a ring of associates who will use them quickly, primarily to buy high-ticket items that can be resold for cash. He gets a cut of the cash they raise in return for his promise to provide more counterfeit cards in the future.

July 28, 2008, Moultrie: Morgan gets her credit card statement in the mail and finds \$4,326 in charges for purchases of consumer electronics and jewelry in several European cities. She immediately calls her credit card issuer and reports the fraudulent transactions to a customer-service representative, who cancels the card and tells Morgan that she need only pay for the purchases she made and that a new card will be mailed to her in a few days.

August 14, 2008, Bangalore: Chandri, nervous about a newspaper account of the busting of an identity theft ring, disconnects his PC, takes it to a dumpster and then buys a new one. He makes no further attempts to steal data from his employer.

February 16, 2010, St. Paul: Watkins gets a call from a local Secret Service office. The agent, Brett Paolini, makes an appointment to talk with him tomorrow.

February 17, 2010, St. Paul: Paolini tells Watkins that a major credit card counterfeiting ring is under investigation and that a substantial number of transactions made at QualitiMart stores were recorded



on the stolen credit cards shortly before the fraud began. He asks for a list of all employees and outsource providers who have access to the database.

March 4, 2010, St. Paul: Paolini brings in forensic experts who check the hard drives of employees at QualitiMart who have access to the database and forwards his report to Washington.

September 18, 2010, St. Paul: Watkins gets another call from

Paolini, telling him that QualitiMart’s data security has been breached, making the retailer liable for as-yet-unknown fraud losses and investigation expenses, in addition to its obligation to notify all of its customers who pay with credit cards about the breach. They must all be warned that their confidential information has fallen into the hands of thieves due to QualitiMart’s failure to enforce adequate security. He hangs up the phone and swears.

May 5, 2011, Bucharest: Elesciue is arrested by Romanian security forces and taken to jail, where he is interrogated by representatives of the U.S. Secret Service.

October 14, 2011, Bangalore: Chandri is arrested by Indian authorities on suspicion of credit card fraud. They have been notified by the U.S. Secret Service that ISP records confirm that a message sent from a library computer activated by his library card proposed selling credit card data. His bank records have been subpoenaed and show a large deposit shortly before a batch of counterfeit credit cards went into circulation.

July 21, 2012, Bucharest: Elesciue is extradited to the United States to stand trial for credit card fraud.

EPISODE TWO

The following account of a data breach is fictional, and all the names are made up, but the details describe the way security breaches do occur in the real world. It was written by Nicholas J. Percoco, vice president of consulting at Trustwave, a Chicago-based data security firm, and by Richard Gamble.

July 17, 2008, Madison, Wisconsin: Juliet Huckaby, a savvy computer hacker, logs on to the Internet, activates her port scanner, and starts the tedious but rewarding process of scanning a range of IP addresses, looking for open ports. She finds one with the URL of portobello3@aol.com and recognizes the remote access software as a 2002 version of a popular program she has encountered before. She tries to get in but hits a password prompt. She suspects an Italian restaurant, so she tries 30 or 40 different words, finally hitting pay dirt with “antipasto.” She’s in and exploring files from the POS system. It’s a new, PCI-compliant POS system, so no credit card data has been stored. But that doesn’t stop her. She implants a keystroke logger, turns off the computer, and unmutes the TV.

July 19, 2008, Grand Junction, Colorado: John Correlli unlocks his restaurant, turns on the oven and starts preparing lasagna. The lunch crowd is light that day due to rain, but Portobello fills for dinner by 7 p.m. and stays busy until 10:30. Many diners pay with credit cards, which are swiped at the cash register.

July 20, 2008, Madison: Huckaby goes back to Portobello's Web site and logs in into the system with the password. She finds that her keystroke logger has worked. When cards were swiped, the logger picked up the mag stripe data just as if they had been entered from a keyboard. She has track data from 27 credit cards. She goes online and starts shopping.

August 28, 2008, Grand Junction: Corelli gets an earful from Martha Jenkins, who took her daughter and son-in-law to dinner at Portobello three weeks ago and paid with her credit card. Now, that card has been used to buy a bunch of clothes from Lands' End. She admits that she used the card at five other local businesses that month, and Corelli assures her that his systems are secure.

September 9, 2008, Madison: Huckaby goes back for another load of data captured by her keystroke logger. She makes a mental note to acquire some memory-dumping software that will capture anything running in active memory on the system. Then she'll have two ways to capture card data when she penetrates systems. She also thinks she should investigate ways to sell the card data to organized crime rings that will use it to manufacture counterfeit cards. That would be turning her hobby into a business. She is lifting full track data (name, card number, expiration date, and banking code) and she knows there some people would pay good money for that, but she isn't motivated to find them.

October 5, 2008, Grand Junction: Correlli gets a phone call from Secret Service agent Chuck Mathis. His restaurant has come up on a common point of purchase (CPP) list generated by the card brand's security system. That means that Portobello is showing up too often among the legitimate charges made by cards that were later used for fraudulent transactions and reported by cardholders. It looks like he might have a data security breach.

October 8, 2008, Grand Junction: A team of forensic investigators recommended by the local bank come to Portobello early in the morning, well before lunch time, to copy the hard drive from the computer that hosts the card reader. They call later in the day and report that they have found evidence of a keystroke logger, the source of the breach. He will have to pay for the forensic investigation and could be liable for losses caused by the breach. He will have to contact his customers to notify them of the breach. They give him four suggestions for reinforcing his data security.

October 15, 2008, Madison: Huckaby goes back to Portobello and finds that the password has been changed. She assumes that the keystroke logger will have been removed and upgraded security put in place, so she starts scanning for another open port.

March 23, 2009, Grand Junction: Corelli declares bankruptcy, closes his restaurant, and moves to Virginia to live with his daughter.

June 6, 2009, Washington, DC: Secret Service closes the case. Because the money involved was small and because the perpetrator covered her tracks well, they drop the investigation. Huckaby is free to continue her thefts. **TT**

Richard H. Gamble is a contributing writer to Transaction Trends. Reach him at gamble10@earthlink.net.

2008 Electronic Transaction Association Award Winner

"Technology Innovation of the Year-2008"

ORION By 4ACCESS COMMUNICATIONS

Check 21 and Card Processing with One Device

- Total Check Solution**
 - Integrated check reader & imager; Check 21; ACH; authorize; guarantee
- Cards, Cards, Cards...**
 - Credit, debit, gift, loyalty, mag stripe or contactless
- Multi-Merchant Capability**
 - Up to 20 merchants per terminal, with fully independent merchant profiles

New Customer Special: Refer to Promo Code K440 for a discount on your first order. Call now for details.

Go with a Winner! To learn more please contact: **Tony Southard** • tony@4access.com • 888.306.4222 ext: 226