

Managing Identity Theft Risk in Software:

THE NEED FOR SOFTWARE RISK ANALYSIS



The Growing Threat

The Federal Trade Commission (FTC) has reported that identity theft costs the United States \$50 billion to \$60 billion a year², and it is widely considered to be the fastest growing crime in the United States.

Consumers and businesses rely on electronic information systems to store, transmit, and manage their most important, private data. The Forrester quote above underscores that a primary threat to this data is introduced because of security vulnerabilities in the software on which it resides. As e-commerce, online banking, and other Web transactions increase in size and frequency, criminals are finding more incentive in targeting identity-related information for theft. For example, investigations into security breaches at Wachovia and Bank of America reportedly uncovered a scheme in which identity thieves were paid \$10 for every customer account they lifted.³ The threat is clearly extending beyond isolated inconveniences.

Not only is there growing evidence of organized crime online, experts also suspect a rise in targeted attacks sponsored by terrorists and nation-states. Imam Samudra, sentenced to death for his part in terrorist bombings in Bali, urged fellow radicals to take the holy war into cyberspace by attacking U.S. computers, "with the particular aim of committing credit card fraud," according to the Washington Post, which also reports that a chapter in Samudra's autobiography provides an outline on how attackers can get started hacking.⁴

Public Cases Raise Awareness of Attacks and Costs

While not a new problem, security breaches in 2005-2006 exposed private customer data of high-profile companies such as ChoicePoint, Bank of America, LexisNexis, HSBC, Ameritrade, Time Warner, Ford, and MasterCard, generating negative attention among customers, press, and legislators.

According to Forrester, many financial services firms, including the most trusted ones, have not taken adequate preventative measures to protect their online channels from attackers. It cites an American Banker Online report from July 28, 2004 that a major credit card company had confirmed finding and fixing a flaw on its Web site's "Find A Card" tool that could have facilitated a phishing scam and had taken it out of service. The report also highlights details published in 2004 by the Anti-Phishing Working Group of four increasingly sophisticated "Verified by Visa" phishing scams. According to the Working Group, in December 2004, attackers cross-scripted www.visa.com and overlaid it with a perfectly forged Verified by Visa card activation page. The forged form had data entry fields for a card account number, expiration date, card verification value, and ATM personal identification number and had been linked to the attackers' Web site.⁵

Breaches of customer information can cost organizations valuable customer and partner loyalty, but they may also lead to more direct costs for legal expenses and settlements. BJ's Wholesale Club Inc. found itself in a court battle after being the target of an identity theft attack in 2004. According to the Wall Street Journal, "BJ's faces suits by a number of banks and credit unions for damages after hackers stole as many as 40,000 credit-card numbers of BJ's customers. BJ's has set aside \$16 million to cover its potential losses."⁶ Legal analysis of this case states that the banks must "absorb the costs of notifying cardholders, reissuing cards, and the interruption of business in the interim... the Pennsylvania State Employees Credit Union (PSECU) claims losses approaching \$100,000, while Sovereign bank claims \$500,000 in losses, and Banknorth NA filed suit claiming losses of \$583,000. Meanwhile, CUNA Mutual Group (mutual insurance company for credit unions) alleges it suffered millions of dollars of losses."⁷ Given the reported number of customers affected by the breach, PSECU's costs averaged \$4.90 for each one whose information had been stolen.

The Wall Street Journal reported that BJ's has tried to shift liability to IBM, claiming that the company supplied credit card transaction software that did not meet agreed-to security

Millions of identities with accompanying financial information are stolen each year through application security vulnerabilities.

Forrester Research¹

requirements. Because of this breach, Visa has started checking software that conducts credit card transactions and approving those that meet standards for how sensitive information is handled.⁸

Despite the recent rise in publicly acknowledged identity theft occurrences and resulting costs, the problem is likely much more commonplace than consumers or organizations realize. Security and law enforcement professionals are still unclear how many incidents of this nature go unreported.

Liability Concerns

To increase nationwide awareness of identity theft incidents, several nationwide bills have been proposed that will pressure companies to assure the protection of sensitive data. One such bill, passed by a House committee in late March, 2006, would require the FTC to regulate minimum information security controls for entities that store personal customer data. Among these controls are processes for “identifying and assessing any reasonably foreseeable vulnerabilities” and “taking preventive and corrective action to mitigate against any vulnerabilities identified.”⁹ Companies not meeting these requirements would likely face fines and other penalties, potentially including civil damages. “Congress is primed to take a very serious look at this and pass comprehensive legislation,” said Sen. Charles Schumer, D-NY, in an interview with the Associated Press regarding identity theft. “Nobody has given this problem the focus it deserves.”¹⁰

Federal regulations have already established a degree of control over the protection of certain types of data. The Health Insurance Portability and Accountability Act (HIPAA) was passed in 1996 to safeguard personally identifiable health information by protecting against reasonably anticipated “threats or hazards to the security or integrity of the information” and “unauthorized uses or disclosures of the information.”¹¹ Financial institutions must meet similar requirements outlined in the Gramm-Leach-Bliley Act (GLBA) of 1999, which requires standards primarily “to insure the security and confidentiality of customer records and information.”¹²

To date, the most relevant legal issues for companies suffering security breaches have come from the FTC. In the cases of BJ’s Wholesale, CardSystems, ChoicePoint, and DSW, the FTC mandated each company to implement a comprehensive security program, which will be the subject of third party audits semi-annually for the next 20 years. For CardSystems, it also imposed charges of \$10 million in civil damages and a \$5 million fund to compensate identity theft victims.¹³

With increased public attention and legislative focus, it is becoming increasingly likely that firms responsible for oversights that lead to theft of customers’ identities will face more than public backlash. Combined with losses in customer trust and brand image, liability concerns are strengthening the business case in all industries for tighter protection against identity theft.

Problems with Software

Vulnerable software continues to be one of the most common weaknesses exploited by criminals targeting personal information. In reports of the privacy breaches at BJ’s Wholesale, CardSystems, ChoicePoint and DSW, the FTC named specific lapses in security on which it based the imposed penalties, including:

- Storing consumer information in unencrypted files
- Unnecessarily storing consumer information
- Not using readily available security measures to limit access between computers on the network and the Internet
- Not adequately assessing the vulnerability of computer networks to commonly known or reasonably foreseeable attacks, including “Structured Query Language” (SQL) injection attacks

The FTC settlements even suggested that the companies were penalized not because they were

“Congress is primed to take a very serious look at this and pass comprehensive legislation... Nobody has given this problem the focus it deserves.”

Senator Charles Schumer, D-NY

"The steady stream of disclosures that customer information is being lost or stolen from retailers has caused security experts to focus on two areas: poor security practices by the retailers themselves and weaknesses in the software used to process credit-card payments."
Information Week

breached, but because they "failed to provide reasonable and appropriate security for sensitive consumer information."¹³ Software vulnerabilities certainly are not the only way sensitive information is exposed, however they are becoming a much more common target for hackers motivated by identity theft.

Between February 15 and June 29, 2005, the Privacy Rights Clearinghouse estimated that publicly-reported identity theft cases exposed the personal information of an estimated 50 million individuals. Of several types of breach, including lost back-up tapes and stolen computers, hacking was the most common method, blamed for nearly half of the reported incidents. In the ten months following that time, hacking was reported an average of nearly four times a month as the cause of a major public security breach.¹⁵

An April 2005 InformationWeek article emphasizes the threat due to software problems, stating that, "the steady stream of disclosures that customer information is being lost or stolen from retailers has caused security experts to focus on two areas: poor security practices by the retailers themselves and weaknesses in the software used to process credit-card payments." The article reports that Polo Ralph Lauren Corp. blamed a software glitch for a security breach that prompted HSBC North America to notify holders of its General Motors-branded MasterCard that their personal information may have been stolen.¹⁶

Solutions

As organizations struggle to avoid being the next victim of targeted attack and public exposure, Forrester outlines the four fundamental steps toward combating IT-fraud and identity theft:

Start at the top with a compliance officer. Make someone responsible for data protection and privacy.

Instill security and standards within applications. Strong authentication and authorization is useless if the application and its data can be compromised directly through application layer vulnerabilities. Security should be integrated into the system development life cycle for applications to limit application vulnerabilities.

Implement identity management. Identity management solutions provide a framework for managing and enforcing policies for people's access to sensitive data.

Enforce a tough audit program. Create and enforce a strong audit and monitoring program. Let employees know that the organization monitors its IT systems and that security infractions will be enforced according to policy — criminal activity will be prosecuted.¹⁷

Because of their posture as highly-lucrative targets, financial institutions have led the way in initiatives combating software-related identity theft. Visa and MasterCard published requirements that took effect on June 30, 2005 for all member institutions, merchants, and service providers that store, process, or transmit cardholder data. This Payment Card Industry (PCI) Data Security Standard requires partners to develop and maintain secure systems and applications and to prevent "common coding vulnerabilities in software development processes."¹⁸

Comprehensive software audits are necessary to identify and remediate these types of flaws in software – such as buffer overflow, privilege escalation, and cross-site scripting vulnerabilities – that allow hackers to access privileged customer data. Companies have found that analyzing the software source code is the most efficient way to pinpoint the root causes of these vulnerabilities and take appropriate steps to protect against attack. Forrester offers this recommendation for addressing cross-site scripting (XSS), one of the most common applications vulnerabilities: "The best way to find XSS flaws on a Web site is to perform a comprehensive and preferably independent

expert security review of the code, searching for all places where input from an HTTP request could possibly make its way into the HTML output. To mitigate the risks effectively, the review must address all applications, including those unrelated to online banking, payment, or card business, such as product catalogs, exchange rates, or branch locators.”¹⁹

The Ounce Advantage

Ounce Labs offers organizations a way to automatically audit their software in order to certify adherence to security policies and identify areas of potential vulnerability. By scanning the source code itself, this technology generates a practical, reliable security assessment of software in legacy systems or during development. It allows companies to set and enforce strict requirements for software security controls, including those found by the FTC to be lacking among the major companies that were breached in 2005.

Specifically, Ounce enables customers to:

- Certify the proper use of accepted software security features, including encryption, access control, authentication, error handling, and centralized logging.
- Identify source code programming errors and design flaws that may expose critical systems to attacks such as cross-site scripting, buffer overflows, race conditions, and privilege escalations.
- Direct remediation and security decisions in the most efficient manner possible to reduce exposure to potential attacks on customer and business data.
- Generate detailed audit reports demonstrating security levels and remediation progress for customers, vendors, internal auditors, and regulatory bodies.

¹Penny Gillespie and Michael Rasmussen, “Combating Fraud in Financial Services,” Forrester, April 7, 2004

²Federal Trade Commission, “Identity Theft Survey Report,” prepared by Synovate, September 2003.

³Wachovie and BofA Notifying Customers of Security Breach,” Paul Nowell, Associated Press, May 16, 2005

⁴“An Indonesian’s Prison Memoir Takes Holy War Into Cyberspace,” Alan Sipress, Washington Post Foreign Service, December 14, 2004

⁵Ivan Remsik, “Secure Online Card Activation Isn’t,” Forrester, April 14, 2005

⁶“Thieves get buyer info stored when card is used,” David Bank, The Wall Street Journal, April 28, 2005

⁷“PSECU v. BJ’s Wholesale,” Ethan Preston, JD, <http://www.eplaw.us/news/>, May 22, 2005

⁸“Thieves get buyer info stored when card is used,” David Bank, The Wall Street Journal, April 28, 2005

⁹H.R. 4127: Data Accountability and Trust Act (DATA), Introduced Oct. 25, 2005, Sponsor: Rep. Clifford Stearns (R-FL), <http://www.govtrack.us/congress/billtext.xpd?bill=h109-4127>

¹⁰“Congress Renews Interest in Identity Theft,” Ted Bridis, Associated Press, April 17, 2005

¹¹Health Insurance Portability and Accountability Act, Public Law 104-191, August 21, 1996

¹²Gramm-Leach-Bliley Act, Public Law 106-102, November 12, 1999, Section 501

¹³Federal Trade Commission, Privacy Initiatives, <http://www.ftc.gov/privacy/index.html>

¹⁴Ibid.

¹⁵Privacy Rights Clearinghouse, source: <http://www.privacyrights.org/ar/ChronDataBreaches.htm>

¹⁶“Customer Data Losses Blamed On Merchants And Software,” Steven Marlin, InformationWeek, April 28, 2005

¹⁷Penny Gillespie and Michael Rasmussen, “Combating Fraud in Financial Services,” Forrester, April 7, 2004

¹⁸Payment Card Industry (PCI) Data Security Standard, source: https://sdp.mastercardintl.com/pdf/PCD_Manual.pdf (Section 6.5.4)

¹⁹Ivan Remsik, “Secure Online Card Activation Isn’t,” Forrester, April 14, 2005

