Data Leakage: The Insidious Threat

Faith M. Heikkila

Data leakage is a silent threat. Employees as insiders can intentionally or accidentally leak sensitive information. This sensitive information can be electronically distributed via e-mail, Web sites, FTP, instant messaging, spreadsheets, databases, and any other electronic means available – all without the knowledge of the organization. The trust placed in employees who are authorized to work with sensitive information is commonplace in all industries. However, the dissemination of sensitive information maliciously or unintentionally can have devastating consequences for the customer, as well as the organization.

A case in point, TJX Companies started off 2007 with the announcement that over 45 million customers' personally identifiable information (PII) had been exposed to hackers for a number of years. As more information was supplied, the number of potentially affected customers grew larger. The credit card issuing banks filed a lawsuit against TJX Companies, citing millions of dollars in damages due to the reissuance of credit cards for the customers of the 2,000 retail stores run by TJX Companies.

Security Breach Notification Laws

In 2007, a number of states followed California SB1386 in promulgating their own security breach notification laws. Michigan became the 35th state and the last of the Great Lakes states to enact a security breach notification law. This new law (2006 PA 566 – amending 2004 PA 452) went into effect on July 2, 2007. There are currently 36 states with security breach notifications laws (http://www.crowell.com/pdf/SecurityBreachTable.pdf). These laws regulate the specific requirements necessary to notify customers of a possible PII security breach and outline the monetary penalties for failure to provide notice. Based on these laws, TJX Companies had to notify their entire customer base of their security breach.

PII is typically defined as a combination of first name or first letter of first name with last name and any of the following: social security number (SSN), driver's license number, telephone number, address, credit or debit card number, bank account number, personal identification number (PIN), password, or username with password. If bank records are compromised by unauthorized access, which could include the unauthorized access by an employee without appropriate permission rights to access files containing PII, a security breach incident has occurred. Adequate notification is necessary after the determination has been made that this data is in fact in the wild. Typically, consultation with an expert or attorney is necessary to determine if the PII has been inappropriately exposed to unauthorized persons. In the event that an employee without the correct credentials accesses the information, it must be verified whether or not they have released any details from such access into the public domain in order to determine if notice to affected customers is required.

FFIEC and FDIC Guidelines for Financial Institutions

As banking customers, we all want the confidentiality, integrity, availability, and non-repudiation of customer information protected. In 2005 The Federal Financial Institutions Examination Council (FFIEC) issued guidelines for safeguarding high risk transactions, such as online money transfers, with the expectation that financial institutions would comply by January 1, 2007. Security breach incidents became more prevalent in 2007 as more and more security breach incidents made national news headlines. As a result, FFIEC regulators have become more concerned with the integrity of online banking systems.

The FFIEC guidelines mandate that financial institutions develop an appropriate security program by utilizing a risk assessment, followed by the use of authentication appropriate for the level of risk. The FFIEC states that single-factor authentication is clearly an unacceptable control mechanism for high risk transactions involving personally identifiable customer information. Hence, it is suggested that multi-factor authentication, multi-layered (defense-in-depth) security, and other controls reasonable to mitigate risk be implemented. Additionally, the FDIC (Federal Deposit Insurance Corporation) and FFEIC have supplemented red flag regulations to

its guidelines.

Red Flag Rules

As a result of the propagating identity theft market, wherein the stakes have been raised by organized crime entering the playing field, the FDIC drafted a supervisory policy on identity theft that was issued on April 11, 2007. On October 31, 2007, the Federal Trade Commission, FFIEC, FDIC, and NCUA (National Credit Union Administration) sent the *Identity Theft Red Flags and Address Discrepancies under the Fair and Accurate Credit Transactions Act of 2003* to the *Federal Register* for publication of the final rule. These red flag rules have a mandatory compliance date of November 1, 2008 by all financial institutions.

The red flag rules require financial institutions to implement a written identity theft prevention program and take specific steps to prevent identity theft. The financial institution must track events to develop patterns of identity theft as an early warning system to proactively notify their customers and the appropriate authorities. Examples of specific events that financial institutions should monitor as possible indicators of identity theft are suspicious or unusual account activity that is inconsistent with previous account activity, consumer fraud alerts received from a consumer reporting agency, suspicious identification documents that appear to be altered or forged, and suspicious access to PII.

Multi-factor Authentication Techniques, Processes, and Methodologies

The chosen financial institution multi-factor authentication solution chosen should be interoperable, reliable, scalable for future growth, and readily accepted by the customers. Additionally, it should be appropriate for the level of risk. The three factors related to authentication methodologies are: something a person knows, something a person has, and something a person is. The following multi-factor authentication methods can be considered by financial institutions for their online banking systems.

Something a person knows:

Shared Secrets
Shared by both institution and customer offline
Faces

Challenge question verification techniques
Positive verification
Logical verification
Negative verification

Out-of-band Authentication
Relatively inexpensive
Authenticated through a second medium such as a cell phone, telephone, fax, or e-mail message
Cumbersome for customer

Something a person has:

Tokens
Costly to distribute
Forget or lose token
USB tokens
Smart Card
Password-Generating Token – one time password changes usually every 60 seconds

Non-Hardware based one-time password scratch card
Less costly
Low tech, easy to use
Bingo Card
Choose character randomly from cell in grid

Internet Protocol Address location
Match IP addresses previously used with customers
Use of public access point in airport or hotel not available
Traveling – difficulties using this technology
Privacy issues

Device Authentication
Authenticates the computer being used is in fact the customer's computer

Geo-location
Calculates location
Not suitable for wireless connection

Mutual Authentication
Digitally signed certificates to authenticate the financial institution's Web site
Digitally signed certificates to authenticate the customer
Certificate Authority (CA) issuing the certificates can be financial institution or a third party CA

Something a person is:
Biometrics
Costly
Reliability issues – false positives and false rejections

Privacy issues with providing personal biometrics – how will they be protected
Fingerprint recognition
Face recognition
Iris recognition
Voice recognition
Keystroke recognition
Handwriting recognition

Data Leakage Security Policy

One new security policy that should be developed is the Data Leakage Security Policy. This policy should prohibit the removal of sensitive customer information in any format (hard copy or electronic) from the premises of the organization. Certain exceptions may be applied; however, this information must then be encrypted. This policy should also restrict the downloading of the entire sensitive member information or PII database. This policy should also include the requirement to log the data being removed for legitimate business purposes. There should be a section in the policy requiring the monitoring and filtering of outbound content to prevent data leakage. This monitoring will provide an audit trail of who downloaded sensitive member content, when, and onto what devices. Should these portable devices be lost or stolen, if they are encrypted and the encryption key has not been compromised, no notice is necessary under the regulations.

One area that is often overlooked in this policy is the requirement to include a contractual obligation in third party agreements mandating that service providers appropriately secure and protect sensitive member information and/or PII. The third party service provider must provide adequate evidence that they have had a security risk assessment of their own hardware and should agree to protect the financial institution's sensitive customer data. Limited access to customer PII as well as the requirement for an escort from the financial institution during any access to such information should be outlined in the agreement and enforced. Another aspect of this policy should be the proper disposal of sensitive member information by deleting/shredding electronic files and documents from laptops, BlackBerrys, PDAs, CDs/DVDs, flash drives and any other portable or removable media. Any PII in hard copy should be secured in locked shred bins and shredded using cross-strip shredders by trusted employees prior to leaving the building. The final component of this security policy should be mandatory training sessions for all employees on how to handle PII on an ongoing basis.

Enforcement of Data Leakage Security Policies

How do you know when an incident of data leakage has occurred? Unfortunately, it is often after the fact that you learn of a data leakage. However, there are automated tools available for purchase to identify, monitor, block, and report when sensitive member information or PII is being transmitted to an unauthorized account or person.

To assist with the enforcement of this security policy, create defense-in-depth by employing numerous software programs and hardware appliances, such as:

- Encryption
- Firewalls
- Intrusion detection systems (IDS) and/or Intrusion protection systems (IPS)
- Virtual private networks (VPNs)
- Content monitoring and filtering (CMF)
- Security events management
- Anti-virus protection

The Gartner *Magic Quadrant for Content Monitoring and Filtering and Data Loss Prevention* for the second quarter of 2007 reported that while data leakage products matured over the past year, they are basically still an adolescent market. One of the leaders identified by Gartner is Vontu, who was recently acquired by Symantec. Websense and Vericept are the other two companies identified by Gartner as data leakage leaders. With these data leakage products, an attempted e-mail message containing a SSN or credit card number is stopped from being sent out and the sender is sent a reminder indicating that content in this e-mail violates federal laws and the financial institution's security policies. This reminder assists with training the employee as to what is acceptable pursuant to the data leakage policy.

Conclusion

Data leakage is an issue that is not going to disappear any time soon. Due to the ubiquitous nature of connectivity and the popularity of portable devices, the usage of this technology for online financial transactions is steadily increasing. Regulatory groups will continue to create laws to police financial institutions; however, the federal regulatory groups want the financial institutions to take the lead and demonstrate their willingness to protect PII at a higher standard than they are required to implement. In many instances, this has already begun, since customers are demanding it and no one wants to have negative press concerning their financial institution in the news.