PIVOTGROUP
SOLUTIONS TAILORED, NOT RESOLD.

Data Leakage: What You Need to Know

by Faith M. Heikkila, Pivot Group Information Security Consultant

Data leakage is a silent type of threat. Your employee as an insider 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 your knowledge.

1. NCUA Appendix B to 12 CRF Part 748 - Guidance on Response Programs for Unauthorized Access to Member Information and Member Notice, (November 2005)

   a. ***Sensitive member information*** **is defined as the member's:**
      i. Name
      ii. Address
      iii. Telephone number
      iv. Social Security number (SSN)
      v. Driver's license number
      vi. Account number
      vii. Credit or debit card number
      viii. Personal identification number (PIN)
      ix. Password
      x. Username along with password
      xi. Account number in conjunction with password (p. 748-8)

   b. **Response program components**
      i. Assess nature and scope of an incident
      ii. Notify the appropriate NCUA regional director or applicable state supervisory authority
      iii. Notify local law enforcement agencies consistent with NCUA's Suspicious Activity Report requirements
      iv. Take appropriate steps to contain and control the incident
      v. Notify members when necessary (p. 748-7)

   c. **Member notice**
      i. Notice must be given to customers as soon as incident discovered
      ii. Timely notice is part of affirmative duty to protect sensitive member information
      iii. Responsible for notice of third party service providers' incidents as well
      iv. Notice may be delayed for criminal investigations with law enforcement written request but not for inconvenience or embarrassment
      v. Credit union must investigate breach and calculate the likelihood of information being used for nefarious purposes (p. 748-8)

d. **Content of member notice**
   i. Description of incident
   ii. Credit union's response
   iii. Credit union hotline for customers with questions
   iv. Request customer inform credit union of any identity theft over the next 2 years
   v. Request customer to also report suspicious account activity to credit union immediately
   vi. Place victim names in fraud notice on credit reporting services
   vii. Recommend obtaining free yearly credit reports
   viii. Provide Federal Trade Commission (FTC) identity theft guidance found on Web site and through telephone contact numbers
   ix. Prior to sending out massive notices to affected credit union customers, credit union should contact consumer reporting services for appropriate contact information to be provided (p. 748-8 – 748-9)

2. *Gramm-Leach-Bliley Act § 501(b) Protection of Non-Public Personal Information* (October 1999)
   a. Title V of GLB focuses specifically on privacy and the protections of member data.
      i. It required specific privacy and security measures be in place at financial institutions by July 1, 2001.
      ii. The act applies to all national banks and the federal branches of foreign banks that are subject to the supervision of the Federal Reserve System, the Office of Thrift Supervision, the Office of the Comptroller of the Currency, or the Federal Deposit Insurance Corporation.
   b. **Section 501 of Subtitle A of Title V, entitled Protection of Nonpublic Personal Information**,
      i. Limits the instances in which financial institutions may disclose nonpublic personal information about a member to nonaffiliated third parties,
      ii. Requires them to disclose certain privacy policies and practices as well as establish safeguards to protect that information.
   c. **Subtitle A, Section 501a states:**
      i. Each financial institution has an affirmative and continuing obligation to respect the privacy of its members
      ii. And to protect the security and confidentiality of those members' nonpublic personal information.
   d. **Subtitle B, Section 501b states**:
      i. Each agency shall establish appropriate standards for the financial institutions within their jurisdiction relating to administration, technical, and physical safeguards:
         1. To insure the security and confidentiality of member records and information;
         2. To protect against any anticipated threats or hazards to the security or integrity of such records; and
         3. To protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any member.

How do you protect sensitive member information and keep your credit union out of the news? 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.

1. **Case in point - May 2006, the Veterans Affairs (VA) office in Washington, D.C. experienced data leakage. This is the VA announcement that appeared on their Web site on May 23, 2006:**

   > The Department of Veterans Affairs (VA) has recently learned that an employee, a data analyst, took home electronic data from the VA, which he was not authorized to do. This behavior was in violation of our policies. This data contained identifying information including names, social security numbers, and dates of birth for up to 26.5 million veterans and some spouses, as well as some disability ratings. Importantly, the affected data did not include any of VA's electronic health records nor any financial information. The employee's home was burglarized and this data was stolen. The employee has been placed on administrative leave pending the outcome of an investigation (http://www.va.gov/index.htm).

2. **Create Data Leakage Security Policies and Conduct Employee Training**

   a. Develop security policies
      - i. Prohibiting the removal of sensitive member information in any format (hard copy or electronic) from the premises
      - ii. Certain exceptions may be applied; however, this information must then be encrypted
      - iii. Restrict the downloading of the entire sensitive member information database
      - iv. Require third parties, such as service providers, to contractually secure and protect sensitive member information

   b. Enforcement of security policies and procedures
      - i. Log the data being removed for legitimate business purposes
      - ii. Monitor and filter outbound content to prevent data leakage
      - iii. Audit trail of who downloaded sensitive member content, when and on to what device
      - iv. Properly dispose of sensitive member information by deleting/shredding files and documents from laptops, Blackberrys, PDAs, CDs/DVDs, flash drives and any other portable or removable media
      - v. Mandatory training sessions for all employees on how to handle sensitive member information on an ongoing basis

3. **Create Defense-in-Depth by employing numerous software programs and hardware appliances**

   a. Encryption
   b. Firewalls
   c. Intrusion detection systems (IDS) and/or Intrusion protection systems (IPS)
   d. Virtual private networks (VPNs)
   e. Content monitoring and filtering (CMF)
   f. Security events management
   g. Anti-virus protection

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 in place to identify, monitor, block, and report when sensitive member information is being transmitted to an unauthorized account or person.

According to the February 17, 2006 Gartner report, *Magic Quadrant for Content Monitoring and Filtering 2006,* products for content monitoring and filtering (CMF) for data leakage are an adolescent market with much growth to be expected over the next two years through acquisitions and new vendors entering the market.

The February 17, 2006 Gartner Report lists the following vendors with products as of November 1, 2005.

VENDOR/ PRODUCT	GARTNER CLASSIFICATION	STRENGTHS	IMPROVEMENTS
Vontu	Leader	Network filtering and endpoint scanning – Scalability, manageability, and accuracy per independent references	Must continue with innovation, increase sales, and develop technical partnerships
Proofpoint	Challenger	Secure e-mail boundary market technology	Inhibited by e-mail roots thereby offering little innovation or leadership in CMF market
Tablus	Visionary	First provider of fingerprinting unstructured data – network filtering, endpoint scanning, and desktop/laptop filtering	Needs to expand client base, as well as complete user interface and endpoint integration
Vericept	Visionary	First CMF vendor on market – network filtering – significant client base established with stable revenue streams	Needs to add filtering capabilities, more integration with e-mail, and more detection techniques
Fidelis Security Systems	Niche player	Newest on the market – only one to offer all-channel blocking via TCP resets	Expand product capabilities
Intrusion	Niche player	Focuses completely on credit unions and provides a compelling turnkey solution – only public company in the CMF Magic Quadrant	More competitive in other general markets
Palisade Systems	Niche player	Combined IPS and CMF – relatively small vendor	More directly target the CMF market – currently targets single-box solution enterprises
Port Authority Technologies	Niche player	Network filtering – a small Israel-based with good document fingerprinting along with good e-mail integration, HTTP filtering – First product to monitor/block internal e-mail	Offer a passive TCP/IP monitor
Reconnex	Niche player	Network filtering – CMF to capture full forensic information of inbound and outbound traffic in a database	Integrate with e-mail systems and offer cross-channel blocking

Since we are technology neutral, Pivot Group can assist you with developing a security program to help you fight data leakage. Pivot Group provides data leakage risk assessment and a solution selection & implementation. Each risk assessment and solution is customized to match the needs of the particular credit union.

1. look, plan, act, repeat

   - look – business assessment of your needs through a risk assessment
     - Identify Critical Member Information
     - Identify the threats and vulnerabilities to the confidentiality, integrity, and availability of Critical
       Member Information
     - Evaluate the likelihood, and impact of threats occurring
   - plan – build a proactive strategy
     - Identify how to mitigate data leakage risks
     - Technical Controls
     - Management Controls
     - Operational Controls
     - Draft or revise data leakage security policies to cover these risks
     - Train employees and customers
     - Develop effective Monitoring, Alerting, & Reporting procedures & techniques
   - act – take action on the plan
     - Implement the controls and recommendations to mitigate vulnerabilities found
     - Revise security policies as necessary
     - Train customers and employees on data leakage security best practices
     - Monitor, Review, & Report activities on a regular basis
   - repeat – the life cycle of information security is a process not a destination
     - Ongoing basis – repeat it on a regular basis as best practices indicate
     - Schedule yearly risk assessment
     - As new technology is deployed, schedule a risk assessment
     - When there is a security breach, schedule a risk assessment

2. **Pivot Group Data Leakage Detection Solution using Open Source Tools**

   - Enhances NCUA Reg. 748 Part B compliance by inspecting traffic outbound to the Internet looking for confidential data (typically personal identifying information)
   - Captures frames containing plaintext confidential data for forensic investigation
   - Alerts administrators when confidential data is outbound in plain text
   - Tracks encrypted connections to the Internet
   - Stores alerts in a database with GUI retrieval capabilities
   - Monthly reports created that contain summary statistics
   - Hardened appliance, hidden network tap deployment, minimal configuration required
   - Easily integrated with new or existing Snort IDS

Faith M. Heikkila is a Pivot Group Security Consultant and currently a Ph.D. Candidate in Information Systems – Nova Southeastern University specializing in information assurance. She has over 18 years of paralegal and IT Project Management experience with two law firms in Michigan. She is a member of Association for Computing Machinery (ACM), Association of Information Technology Professionals (AITP), Computer Security Institute (CSI), Institute of Electrical and Electronics Engineers, Inc. (IEEE), Information Systems Security Association (ISSA).