Data Loss Prevention: Considerations from an IT Audit Perspective

ISACA November Luncheon

11 November 2010

ERNST & YOUNG
Quality In Everything We Do
Agenda

► What is data loss prevention (DLP)?
► Ernst & Young point of view on DLP
► Data loss risk assessment
► Moving forward after the DLP risk assessment
► Case studies and examples
What is DLP?

Defining the concepts

► Data loss and data leakage — what does it all mean?
► How does it occur?
► Why does it occur?
► What is the end result?
► What are DLP solutions intended uses?
It’s all about the data

- Data is the most valuable asset for many companies and must be protected as such.
- New business and technology paradigms force a shift from reliance on traditional perimeter security to data level security and controls.

<table>
<thead>
<tr>
<th>Compliance</th>
<th>Intellectual Property</th>
<th>High Business Impact (HBI) Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>SOX</td>
<td>Customer Lists</td>
<td>Board Minutes</td>
</tr>
<tr>
<td>HIPAA</td>
<td>Price/Cost Lists</td>
<td>Financial Reports</td>
</tr>
<tr>
<td>PCI</td>
<td>Target Customer Lists</td>
<td>Merger/Acquisitions</td>
</tr>
<tr>
<td>GLBA</td>
<td>New Designs</td>
<td>Product Plans</td>
</tr>
<tr>
<td>FISMA</td>
<td>Company Logo</td>
<td>Hiring/Firing/RIF Plans</td>
</tr>
<tr>
<td>ITAR</td>
<td>Source Code</td>
<td>Salary Information</td>
</tr>
<tr>
<td>SB 1386</td>
<td>Formulas</td>
<td>Acceptable Use</td>
</tr>
<tr>
<td>Others</td>
<td>Process Advantages</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Pending Patents</td>
<td></td>
</tr>
</tbody>
</table>

What you did not know needed protection:
- Review of Key Employee actions before they announced departure
- Unreported but Important Memos/Reports
- Code names of projects not reported to Security department
Ernst & Young point of view on DLP

Data loss in the news

► Large retail company — 45.6 million credit and debit card numbers were stolen over a period of more than 18 months
► Large BCBS insurer — 57 hard drives containing member-protected health information were stolen
► Department of Commerce — an employee inadvertently transmitted over the Internet an unencrypted file containing the personally identifiable information (PII) of Commerce employees to other department employees
► A medical center in Kentucky is notifying 5,418 patients of a breach resulting from the theft of an unencrypted portable hard drive stored in a locked area
► FTC Consent Decree requires monitoring and filtering of outbound computer traffic to block export of sensitive information
► More than 250 privacy laws that mandate disclosure of data breaches
► 2% of laptop inventory cannot be located
► Fortune 500 companies lose two laptops a day

Sources: engadget, Computerworld and CNET news.
More than half say protecting reputation and brand is their biggest information security challenge

64% see the disclosure of sensitive data as one of their top five IT risks

55% indicate they are increasing the level of investment related to their top five areas of information security risk

52% see the use of personal devices as the main cause of an increasing risk of data leakage

50% plan to spend more in the next year on data loss prevention efforts
Ernst & Young point of view on DLP

Common myths and challenges

**Common myths**

- Company does not have any sensitive information that we need to worry about
- Employees are trained and aware of the data loss risks associated with sensitive data
- Data loss can be solved with just a tool implementation
- The space is not very mature and only early adopter companies are investing in DLP

**Common challenges**

- Majority of data loss scenarios are unintentional and inadvertently committed by insiders
- Complexity of information flows within the extended enterprise
- Lack of forensic and incident response capabilities to respond to data loss and data breaches
- Growing number of and complexity of regulatory requirements to protect sensitive information
The cost of a data breach

- Brand damage and loss of reputation
- Loss of competitive advantage
- Loss of customers
- Erosion of shareholder value
- Fines and civil penalties
- Litigation and legal action
- Regulatory action and sanctions
- Significant cost and effort to notify affected parties and recover from the breach

*Data breach incidents cost US companies $204 per compromised record, with an average total per-incident cost of $6.75m – Ponemon Institute*
Data loss risk assessment

What is the goal?

Drivers
1. Loss or theft of laptops and mobile devices
2. Unauthorized transfer of data to USB devices
3. Unable to locate and protect sensitive data
4. Theft of company secrets by employees
5. Print and copy of client data by staff
6. Lack of content awareness and coordinated response to intrusions
7. Access to sensitive files by unauthorized users

Business case

Stakeholders

Recent data loss

Drivers

Business case

Stakeholders

Recent data loss
Data loss risk assessment

Ernst & Young’s use of a leading DLP appliance

► Clients want an independent third party to help in assessing and addressing risks associated with data loss.

► Our Information Security Services has the industry depth to provide clients with information security assistance that is tailored for their industry and company.

► Use of technology for an assessment provides clients with evidence of data loss and provides value when coupled with our knowledge of the client’s company and industry.

Source: Gartner MQ – June 2010
Data loss risk assessment

- Our assessment approach combines our deep data protection, regulatory and compliance experience with the use of a leading DLP technology:
  - Identify critical information types within the enterprise, primary and secondary locations, and communication vectors
  - Monitor data leaving the corporate network using a DLP solution
  - Analyze collected data
  - Provide a report and close-out session providing observations and recommendations aimed at reducing data protection gaps and risks to the enterprise

- At the completion of the assessment, our client understands:
  - Where critical and sensitive information resides in their network
  - How that information is moving throughout their enterprise, over which communications channels, and who is sending and receiving that information
  - Compliance risks in their environment previously not recognized
  - Next steps, “quick wins,” and long-term recommendations to reduce data and business risks
A DLP program must include all domains of people, process and technology to effectively prevent the loss of data.
Case study: international oil and gas company, domestic financial institution, international software company

Client concerns

► Client concerned about data loss and aware of emerging threat industry
► Wanted to build a business case for investing in DLP
► Organization had a low awareness related to data loss and the types of sensitive data on their network
► Company had inconsistent processes related to the management of sensitive data
► Company wanted to see if they had any issues with data loss
► Company wasn’t aware where they had sensitive data stored internally

Ernst & Young solutions and results

► Ernst & Young deployed the DLP appliances to gain a better understanding of the company’s management of sensitive information as it is stored and transferred
► The assessments highlighted weaknesses in the overall DLP program and evidenced the loss of sensitive data such as IP, PII and PHI
► Technology was accompanied with business process assessment to provide process-level root cause for data loss
► Assessment provided CIO, IA, Legal, HR, CFO, Audit Committee, with insight to the company’s data loss exposure and detailed recommendations on how to address DLP
Case study: establish your process before starting

- Make sure Legal and HR are aware of the assessment.

- For the assessment, you are less concerned with getting someone in trouble than stopping the problem.

- You will find something — have a defined process before you start the assessment.
  - Business process failures usually involve escalation within IT and engagement with the business unit itself.
  - Employee violations, due to their sensitivity, require a more formal process. You want to implement whatever process you already have in place for internal employee investigations and potential termination.
Case study: things to analyze

- Top violations by data type
- Top violations by business unit
- Top violations by volume
- False positive patterns
- Different violations from same source
- Unusual origins
Case study: dashboard view
Case study: HR sending sensitive info to webmail

Provides evidence of data loss of sensitive employee information

Oscar [redacted] was confirmed positive for cocaine from the lab. His # is [redacted].

Employee’s name and drug test result sent to a yahoo account.
Case study: employee salary info sent to webmail

Provides evidence of data loss of sensitive employee information
Case study: employee PII sent to webmail

Provides evidence of data loss of sensitive employee information

Multiple employees’ PII clearly listed in this email
Case study: employee PII sent to external party

Provides evidence of data loss of sensitive employee information

<table>
<thead>
<tr>
<th>Original Incident ID</th>
<th>12199</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protocol</td>
<td>SMTP_Request</td>
</tr>
<tr>
<td>Capture Device</td>
<td></td>
</tr>
<tr>
<td>Time Sent</td>
<td></td>
</tr>
<tr>
<td>User ID</td>
<td>Unknown</td>
</tr>
<tr>
<td>Source IP/Port</td>
<td></td>
</tr>
<tr>
<td>Source Location</td>
<td>United State</td>
</tr>
<tr>
<td>Destination IP/Port</td>
<td></td>
</tr>
<tr>
<td>Destination Location</td>
<td>United State</td>
</tr>
<tr>
<td>Policy</td>
<td>SOX Compliance (admin)</td>
</tr>
<tr>
<td>Rule</td>
<td>Compensation and Benefits Related Documents</td>
</tr>
<tr>
<td>Sender</td>
<td></td>
</tr>
<tr>
<td>Recipients</td>
<td></td>
</tr>
<tr>
<td>Subject</td>
<td></td>
</tr>
<tr>
<td>Attachments</td>
<td>attachments file</td>
</tr>
<tr>
<td>Message</td>
<td>Show Message in Separate Window</td>
</tr>
</tbody>
</table>

Please see attached file. included salaries and vacations listed. Also please note file attached.

Note: salary increases effective the 01/07/2010.

Return date for checking the 20th, thanks.

Please ensure the columns and format are the exact same on the payment file as it makes it easier for us when we upload the payments, thank you.

Kind regards,

Multiple employees’ PII clearly listed in this email
## Case study: credit card numbers sent unencrypted

Credit card number used for payment sent in the body of an email

<table>
<thead>
<tr>
<th>ID</th>
<th>38550</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protocol</td>
<td>SMTP_Required</td>
</tr>
<tr>
<td>Source Device</td>
<td></td>
</tr>
<tr>
<td>Time Sent</td>
<td></td>
</tr>
<tr>
<td>User ID</td>
<td>unknown</td>
</tr>
<tr>
<td>Source Location</td>
<td>United States</td>
</tr>
<tr>
<td>Destination IP/Port</td>
<td></td>
</tr>
<tr>
<td>Destination Location</td>
<td>United States</td>
</tr>
<tr>
<td>Policy</td>
<td>PCI Compliance (admin)</td>
</tr>
<tr>
<td>Rule</td>
<td>Unencrypted Mastercard Numbers</td>
</tr>
</tbody>
</table>

### Message

Good Morning

I would like to order the following:

- 10 sheets of Daily stamps in the total amount of $600.00

Please charge my credit card: [Redacted] Please leave the validation stickers and invoice with the package.

Thanks,
Case study: employee PII sent unencrypted

Personal data sheet contains new hire’s social security number

---

We are excited about the prospect of you [redacted] attached the offer letter along with the supporting documents that I mentioned today on the phone. As discussed, a complete employment package should arrive via FedEx this week. Please take the time to review all of the information that will arrive in your package.

If you decide to accept our offer of employment you will need to fax [redacted], email [redacted], or return the requested documents back to us. We will need the entire copy of the signed offer letter (2 pages) and a completed Personal Data Form (1 page). We need only the signature pages of Confidentiality, and Assignment of Inventions Agreement (1 page), the Insider Trading Policy (1 page), and the Code of Business Conduct & Ethics (1 page).
Case study: high-level PII dataflow

Helps to understand business process and root cause of data loss
# Case study: sample analysis of data loss incidents

Provides client with Ernst & Young observations related to what the DLP tools found

<table>
<thead>
<tr>
<th>Observations</th>
<th>Potential root causes</th>
</tr>
</thead>
</table>
| ► Number of incidents: 67  
  ► 44 incidents contained bulk SSN  
| ► Lack of employee awareness  
| ► Content commonly found in:  
  ► Excel documents  
  ► PDF documents  
  ► Word documents  
  ► Text files  
| ► High use of PII in routine business activities  
| ► SSN commonly used as employee identifier  
| ► Attempt to steal employee PII  |

<table>
<thead>
<tr>
<th>Risks to company</th>
<th>Recommendations</th>
</tr>
</thead>
</table>
| ► Identity theft or fraud  
| ► Possible prosecution of company under state privacy laws:  
  ► Subject to fines  
  ► Loss of reputation  
  ► Decline in business  | ► Training and awareness  
| | ► Collect only what you need and can protect  
| | ► Create policies and procedures around accessing and transferring this information  
| | ► Monitor electronic communications for large number of PII  |
# Case study: high-level road map for a DLP program

Provides client with short term and longer-term recommendations to increase their maturity

<table>
<thead>
<tr>
<th>0–2 Months</th>
<th>2–4 Months</th>
<th>4–6 Months</th>
<th>6–12 Months</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>People</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Obtain certification from network users</td>
<td>Create communication plan to notify users of proper use of sensitive data</td>
<td>Define data owners, roles and responsibilities</td>
<td>Develop a formal training and awareness program</td>
</tr>
<tr>
<td><strong>Process</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Acceptable use policy</td>
<td>Assess business processes that collect, use, store and transfer sensitive data</td>
<td>Define sensitive information and identify where it resides</td>
<td>Baseline network traffic for anomaly detection</td>
</tr>
<tr>
<td>Conduct internal and external scans on a periodic basis</td>
<td>Update policies to restrict the use of webmail for business use</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Update policies to restrict the use of webmail for business use</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Technology</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Block all non-business related traffic outbound to high-risk countries, as defined in assessment</td>
<td>Provide guidance and tools to allow users to encrypt sensitive emails that may or may not use TLS</td>
<td>Secure sensitive data and enforce acceptable use policy</td>
<td>Actively manage firewall rules</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Monitor all outbound traffic for sensitive information</td>
<td></td>
</tr>
</tbody>
</table>

Increasing maturity of a company’s DLP program
Conclusion: the benefits of a data protection program

Holistically addressing the data loss problem

Data protection is an umbrella term that describes the program, governance, policy instantiation, management controls and solution implementation of people, process and technology measures to prevent the loss of, or unauthorized access to, sensitive data.

![Diagram showing data protection components]

- **Program components**
  - Personnel security
  - Awareness and training
  - Privacy
  - Asset management

- **Data in motion**
  - Secure data transfer
  - Secure messaging
  - Data loss prevention
  - Data audit and reporting

- **Data in use**
  - Data loss prevention
  - Access management
  - Rights management
  - Data audit and reporting
  - Encryption operations
  - Data redaction
  - Data masking

- **Data at rest**
  - Database encryption
  - Storage/disk encryption
  - Mobile data encryption
  - Data loss prevention

- **Information classification, policies and standards**
  - Data management, audit and reporting
  - Data governance and compliance

- **Program components**
  - Access controls
  - System and network controls
  - Incident response
  - Continuity management

**Employees**, **Contractors**, **Third party**, **Partners**, **Former employees**, **Hackers/competitors**

- Personnel security
- Awareness and training
- Privacy
- Asset management

- Secure data transfer
- Secure messaging
- Data loss prevention
- Data audit and reporting

- Data loss prevention
- Access management
- Rights management
- Data audit and reporting

- Database encryption
- Storage/disk encryption
- Mobile data encryption
- Data loss prevention

- Encryption operations
- Data redaction
- Data masking

- Access controls
- System and network controls
- Incident response
- Continuity management

**Ernst & Young**

*Quality In Everything We Do*
Contact information

Anil Markose CISA, CISSP, CIPP
Senior Manager, Ernst & Young LLP
anil.markose@ey.com
Direct: 214 969 9734
Ernst & Young

Assurance | Tax | Transactions | Advisory

About Ernst & Young
Ernst & Young is a global leader in assurance, tax, transaction and advisory services. Worldwide, our 141,000 people are united by our shared values and an unwavering commitment to quality. We make a difference by helping our people, our clients and our wider communities achieve their potential.

Ernst & Young refers to the global organization of member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit www.ey.com.

About Ernst & Young’s Assurance Services
Strong independent assurance provides a timely and constructive challenge to management, a robust and clear perspective to audit committees and critical information for investors and other stakeholders. The quality of our audit starts with our 60,000 assurance professionals, who have the experience of auditing many of the world’s leading companies. We provide a consistent worldwide audit by assembling the right multidisciplinary team to address the most complex issues, using a proven global methodology and deploying the latest, high-quality auditing tools. And we work to give you the benefit of our broad sector experience, our deep subject matter knowledge and the latest insights from our work worldwide. It’s how Ernst & Young makes a difference.

© 2010 Ernst & Young LLP.
All Rights Reserved.
1010-1200121