Data Loss is only half the story

— Protecting Information is the missing piece
Presenter

- Debra Banning — Global Director, Information Security Center of Expertise
  - B.S. and M.S. in Computer Science
  - 26 years information security experience
  - Broad range of public and private sector clients
  - Started information security career in the penetration testing field back in the 1980’s
  - Deep expertise in governance, strategy, risk management, data protection, penetration testing and social engineering
  - Leads National Practice for Information Security
Today’s Agenda

- **Introduction**
  - Definitions
  - Calibration/De-Calibration

- **Defining the Problem**
  - Impact/Risk of Data Loss
  - High Profile Data Breaches

- **Responding to the Challenge**
  - Data and Information Protection Practices
  - Role of Oversight in Data Protection

- **Discussing the Way Forward**
  - Defining a Data Loss Prevention Program

- **Additional Ways to Approach DLP**
  - Integration with Existing Processes
  - Supporting Services

- **Summary and Closing Remarks**
Introduction to Data Loss Prevention and Information Protection
- Definitions and Calibration
Data or Information – Does it Matter?

**Data**
- Represents real world things, events, transactions, etc.
- Can be characters, sounds, images or motions
- Captures discrete values, but are not necessarily unique
- Relevant within a defined context
- May change over time

**Information**
- Sets of data that have specific organization and meaning to an arbitrary or defined customer/user
- Created by the processing, manipulation, interpretation or presentation of data
- Involves an implicitly or explicitly defined context

*Businesses depend on information to make decisions, and that information is inextricably dependent on the data that constitute the information*
Linking Data and Information Protection

- Data protection is a systematic approach to identifying, monitoring and protecting the confidentiality, integrity and availability of data in motion, at rest or in use
- Aggregated data forms “information” is at the heart of our personal lives and business operations
- It is our “information” that is the target of hackers, organized crime and Nation State threats

For purposes of this presentation data and information will be considered equally important as both require adequate appropriate control measures
Types of Data and Information at Risk

- Intellectual Property / Trade Secrets
- Corporate Strategy
- Unreleased Financial Information
- Personal Health Information (PHI)
- System Data and Configuration Settings
- Personally Identifiable Information (PII)
First, Some Calibration …

Data Protection “Facts” most should agree with

• Every business has critical and non-critical systems and data
  – *But most don’t effectively differentiate data into tiers*

• Business impacts of poor data protection can be serious
  – *More companies are getting in the headlines for data breaches*

• One-size-fits-all data protection is neither prudent nor practical
  – *So most focus on only the mandated control areas*

*Surprisingly, the voice of oversight is often absent in exposing these issues*
...and Some De-Calibration

Data Protection “Facts” most should NOT agree with:

• Data protection is strictly an IT and Information Security responsibility  
  – *Assuming it is someone else’s job removes the obligation to act*

• Data protection is only a requirement for regulated companies  
  – *Data is an asset that needs to be protected in every organization*

• Data protection can’t be achieved in today’s business environment  
  – *Many try to transfer the issues to 3rd party services (e.g., cloud)*

*Organizations need to challenge arguments and excuses for not taking action*
Defining the Problem
- Data and Information Loss Risks and Cost
What are Your Risks?

- Data and information loss can result in:
  - Significant financial penalties
  - Extensive operational impact
  - Increased monitoring costs
  - Adverse publicity
  - Negative effect on brand and reputation
  - Lost business
### Value and Risk of an Organization’s Information

<table>
<thead>
<tr>
<th>Information</th>
<th>Value</th>
<th>Threat</th>
<th>Vulnerability</th>
<th>Counter-measures</th>
<th>Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>Consolidated financial information</td>
<td>$$$</td>
<td>⚤ ⚤</td>
<td>🔴 ⚜️</td>
<td>+ + +</td>
<td>△△</td>
</tr>
<tr>
<td>Customer personal information</td>
<td>$$$</td>
<td>⚤ ⚤ ⚤</td>
<td>🔴 🔴</td>
<td>+ + +</td>
<td>△△△△</td>
</tr>
<tr>
<td>Internal office memorandums (non-confidential)</td>
<td>$</td>
<td>⚤</td>
<td>🔴 🔴 🔴</td>
<td>+</td>
<td>△</td>
</tr>
<tr>
<td>Confidential executive memorandums</td>
<td>$$</td>
<td>⚤ ⚤</td>
<td>🔴 🔴</td>
<td>+</td>
<td>△△</td>
</tr>
</tbody>
</table>

#### LOW
- $  

#### MED
- $$  

#### HIGH
- $$$$
High Profile Data Breach Incidents

• Global Payments, Inc.
  – Press coverage of data loss started March 30, 2012
    • incident occurred on January 21, 2012
    • discovered on March 1, 2012
  – 1,500,000 records – card holder numbers were obtained
  – Card holder names, addresses, and social security numbers were NOT obtained.
  – No known actual costs
  – $90,000,000 Ponemon Institute Direct Costs Estimate

Source: Open Security Foundation / DataLossDB.org
High Profile Data Breach Incidents (Cont.)

- **Sony Corporation – PlayStation Network**
  - April 26, 2011
  - 77,000,000 records – names, addresses, email addresses, birthdates, PlayStation Network/Qriocity passwords and logins, handle/PSN online ID, profile data, purchase history and possibly credit cards obtained.
  - No known actual costs
  - $4,620,000,000 Ponemon Institute Direct Costs Estimate

- **Sony Corporation**
  - May 02, 2011
  - 24,600,000 customer dates of birth, email addresses and phone numbers, including 12,700 non-U.S. credit or debit card numbers and expiration dates and about 10,700 direct debit records including bank account numbers accessed by hacker
  - No known actual costs
  - $1,476,000,000 Ponemon Institute Direct Costs Estimate

*Source: Open Security Foundation / DataLossDB.org*
High Profile Data Breach Incidents (Cont.)

- **TJX Companies**
  - January 17, 2007
  - 94,000,000 credit card numbers and transactions compromised
  - $64,113,000 total known costs
  - $5,640,000,000 Ponemon Institute Direct Costs Estimate

- **US Department of Veteran Affairs**
  - May 22, 2006
  - 26,500,000 -- U.S. military veterans Names, Social Security Numbers, and dates of birth
  - $20,000,000 total known costs
  - $1,590,000,000 Ponemon Institute Direct Costs Estimate

*Source: Open Security Foundation / DataLossDB.org*
Security Flaws Create Risks to Your Data

- Information security strategies and objectives not adequately linked to business goals
- Incomplete governance and leadership involvement
- Ineffective security policies
- Irregular or ineffective security risk assessments
- Lack of awareness regarding location of critical data, how to classify it and how to protect it throughout its lifecycle
- Inadequate monitoring of security controls
- Miscommunication with internal and external audiences regarding security requirements and expectations
- Flawed Web application design — common vulnerabilities persist
- Server and database vulnerabilities
- Ineffective access definitions
- Phishing and social engineering
How Much is your Personal Information Worth?

Black Market Value for Personal Information

- Stolen credit card numbers: $.06 each (for 10,000+); $30 each (for smaller orders)
- Hijacked email accounts: $.10 to $100/account
- Bank account credentials: $10 to $1,000/account (sometimes based on balance)
- CVV2 data sets: $1.50/set

What People Will Pay to Protect Personal Information

- Social Security number/government ID: $240/year
- Credit Card number: $150/year
- Electronic or Physical Histories: $52 - $59/year
- Health Industry Medical Records: $38/year
- On-line buying habits and social profiles: $3 - $5.70/year
- Contact Information (phone number, e-mail or mailing address): $4.20/year

Source: “What’s Your Personal Data Worth” by Tim Money, Jan. 18, 2011, designmind.frogdays.com blog

Source: Experis Research
Responding to the Challenge
- The Role of Governance and Oversight
Governance Considerations

- An important aspect of executing an effective DLP program is the incorporation of Governance activities.
- Key areas to include:
  - Roles and Responsibilities – Responsibilities for all aspects of DLP operations need to be clearly defined within the business units as well as at the Corporate level.
  - Processes – Processes including decision points that integrate with defined roles and responsibilities should be defined for the DLP program.
  - Oversight, Management and Review – Oversight structure should be defined that incorporates a combination of centralized and decentralized (Business Unit) responsibilities.
## Roles and Responsibilities

### Data Loss Prevention

<table>
<thead>
<tr>
<th>Audit Committee</th>
<th>C-Level Executives</th>
<th>Business Operations</th>
<th>Information Security Officer</th>
<th>Information Technology</th>
<th>Internal Audit</th>
<th>All Users and Vendors</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ultimate Accountability</td>
<td>Overall Responsibility</td>
<td>Data Ownership</td>
<td>Guidance and Oversight</td>
<td>Data Custodian and Tool Implementation &amp; Operation</td>
<td>Monitor and Evaluate Operational Effectiveness</td>
<td>Follow policies and guidance and report suspected breaches</td>
</tr>
</tbody>
</table>

**Responding to the Challenge**
The Role of Internal Control in Data Protection

Obligation/Role

- Measure compliance with management’s prescribed policies and procedures
- Promote efficiency and effectiveness of operations
- Safeguard and evaluate the protection of organizational assets
- Evaluate proper data handling by all partners and third-parties

Key data protection questions

- Do systems and services have data protection that ensures the resulting compliance is both sufficient and trustworthy?
- Is critical data identified and labeled accurately across the organization?
- Are all key dimensions of data protection applied effectively to critical assets?
- Do SLAs and third-party assessments adequately address data protection?

In times of change, Internal Control should get proactively involved in the planning process to make sure data protection is properly handled
The Role of Internal Audit in Data Protection

**Obligation/Role**

- Review and report on the management and reporting of key risks
- Identify, assess and report on potential issues with the acceptance of risk and level of residual risk
- Provide independent and objective assurance of risk management, internal control, and governance processes
- Act as the ‘eyes and ears’ of the Audit Committee

**Key data protection questions**

- Are potential risk areas affecting data protection identified and communicated?
- Is operational data integrity sufficient to assure the levels of risk and residual risk are accurate and complete?
- Is there sufficient review of the underlying processes and data to support the level of assurance internal audit must provide?
- Is available control/risk reporting data of sufficient quality to facilitate a full review?

*As the advocate of the Audit Committee, Internal Audit needs to ensure processes are in place to deal with data during organizational changes*
Oversight Can Impact Data Protection in Other Ways

• Ensuring there is routine review of aggregate data in addition to discrete data will provide an alternate perspective on the level of accepted risk and control
• Establishing mandatory root cause analysis and examination of critical anomalies will identify underlying data protection (and service delivery) issues
• Requiring a broader examination of the true scope of identified findings in similar systems and services will expose potential underlying systemic issues
• Establishing annual audit/control review plans that incorporate key elements of data protection will impact tactical and strategic (including M&A) data risks
• Forming an appropriate level of discussion among oversight functions (including internal control, audit, IT, IS, and compliance) will foster a better understanding of risk and more effective elimination of data risks

Oversight Functions are critical participants in achieving good data protection!
Discussing the Way Forward
- Building a DLP Program
Suggested Steps for Creating a DLP Program

- Profile Your DLP Needs
- Characterize Your Current DLP Capabilities
- Assess Your Current DLP Effectiveness
- Define a DLP Strategy
- Create an Action Plan to Achieve the Strategy
Profile Your DLP Needs

Goal: Develop a full understanding of key data types and their uses

Suggested Activities:
- Identify primary DLP business needs and drivers
- Determine primary information asset classes (including Trade Secret, Intellectual Property, PII, PFI and Financial Data)
- Determine primary business, regulatory and customer DLP requirements
- Determine information protection and retention requirements
- Characterize primary and secondary data user groups
- Identify current formal/informal data classifications and extent of use for:
  - Data at Rest
  - Data in Motion
  - Data in Use
Characterize Your Current DLP Capabilities

Goal: Identify and understand all currently implemented components and ongoing initiatives affecting Data Loss Prevention

Suggested Activities:
- Determine maturity levels of processes, procedures and solutions currently deployed that impact DLP, including:
  - Data Classification
  - Data Discovery
  - Data Protection
  - Governance and Risk Management
  - Monitoring, Measurement and Improvement

Current State Capability Maturity Scale

<table>
<thead>
<tr>
<th>Capability Level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>No capability currently exists</td>
</tr>
<tr>
<td>Progressing</td>
<td>Elements of a capability exist and meet some of the compliance requirements and business objectives</td>
</tr>
<tr>
<td>Basic</td>
<td>The capability supports core business processes and compliance requirements</td>
</tr>
<tr>
<td>Advanced</td>
<td>The capability incorporates information security solutions that exceed basic compliance requirements and incorporates industry leading practices</td>
</tr>
<tr>
<td>Industry Leading</td>
<td>The capability exceeds industry standards and sets the model for industry to follow</td>
</tr>
</tbody>
</table>
Assess Your Current DLP Effectiveness

Goal: Determine current security program effectiveness in addressing DLP

Activities:
- Evaluate the effectiveness of deployed information protection components to meet DLP requirements
- Estimate the applicability and potential DLP impact of in-process and planned security initiatives
- Determine critical gaps, improvement opportunities and residual risk levels

Risk Determination Scale

<table>
<thead>
<tr>
<th>Critical</th>
<th>High</th>
<th>Moderate</th>
<th>Low</th>
</tr>
</thead>
<tbody>
<tr>
<td>Extremely weak or non-existent capabilities; likelihood for exploitation of current state is extremely high; risk of severe adverse impact to company assets is critical and requires immediate attention</td>
<td>Limited or poorly implemented capabilities, large gaps exist; likelihood for exploitation of current state is high; risk of serious adverse impact to company assets is high and requires priority attention</td>
<td>Capabilities exist, but lack formality and consistency; likelihood for exploitation of current state is moderate to high; risk of adverse impact to company assets is moderate and may require priority attention</td>
<td>Consistent, integrated and managed capabilities are employed; likelihood for exploitation of current state is low; even with no priority attention, risk of adverse impact to company assets is low</td>
</tr>
</tbody>
</table>
Define a DLP Program Strategy

- **Goal:** Define Objectives to implement Vision and Goals and Finalize Strategy
- **Activities:**
  - Create a vision that resonates with all aspects of the business
  - Define goals that encompass Governance, People, Processes and Technology to be effective
  - Work with data owners and stakeholders to identify objectives across the DLP components as aligned with the goals:
    - Data Classification
    - Data Discovery
    - Data Protection
    - Data Handling
    - Governance and Risk Management
    - Monitoring, Measurement and Improvement
  - Validate and Finalize
Data Loss Prevention Strategy Structure

DLP Strategy Framework

1. DLP Vision
2. DLP Goals
3. DLP Objectives

Characteristics

- Sets out a common long-term picture and strategic direction for the Data Loss Prevention program
- Establishes the core business value to be delivered by the Data Loss Prevention program
- Identifies common and business specific goals that reflects each aspect of the vision
- Encompasses both immediate and future direction across the enterprise
- Integrates measurable targets and procedures for evaluating the progress against specified goals and objectives
Develop a DLP Program Action Plan

Goal: Create a DLP Program Action Plan to close current gaps and implement the defined DLP strategy

Activities:

- Develop Action Plan, which typically includes:
  - Workstream Overview
  - “Quick Win” Activities
  - Prioritized Implementation
  - Responsible Parties
  - Resource Estimate
  - Cost Range
  - Execution Timeline
  - Critical Success Factors
Common Mistakes in Planning a DLP Program

• Looking for the “silver bullet”
  – *Installing a DLP tool will not solve the problem*

• Having an isolated project or team rather than a holistic approach
  – *Collaboration is required for a successful DLP program*

• Lack of sponsorship
  – *DLP requires senior management commitment*

• Treating it like a compliance project
  – *DLP must be integrated into the business processes*

• Not building the appropriate foundation for the program to work
  – *Effective DLP requires people, processes and technology*
Additional Ways to Approach DLP
- Integration with Existing Processes and Services
Integrate DLP with ILM Processes

- Linking DLP to an information lifecycle is a proactive means to eliminate problems BEFORE they impact data.
- Incorporating continuous improvement into processes ensures new issues will be identified and corrected.
- The PDCA (Plan-Do-Check-Act) process overlay can also be used to link DLP and ILM to security management processes.

**DLP should be integrated into every aspect of your organization’s Information Lifecycle Management process - from creation to destruction.**
Integrate DLP with Enterprise Risk Management

- Incorporating DLP practices into risk management ensures risks are consistently assessed and evaluated
- Better definition of data classification and protections needed can also improve the resulting risk clarity and completeness
- The ERM process can be directly linked to the PDCA process typically used to evaluate and manage data protection
- Formalizing the link will reduce the potential for risk prioritization disconnects

Integrating DLP into enterprise risk will help ensure the effectiveness, completeness and accuracy of the risk decisions
Integrate DLP with IT Systems Management

Integration of DLP with IT Systems Management

- **IT designs and delivers the core technology, processes and applications that create and manage the data** – which makes this the ideal place to address DLP
- **In many organizations, the software lifecycle that drives applications has already incorporated security and data integrity controls**
- **This process area can accommodate the same PDCA continuous improvement process used to drive sustainable improvements elsewhere**

*Integrating DLP practices into systems management enables the business to address DLP issues at their origin – when the data is created*
Include Data Protection in Employee Awareness

- Employees are critical to a successful data management and data loss prevention program
- Employee awareness programs need to include:
  - Overall DLP Policy and supporting policies (e.g., Acceptable Use)
  - Initial DLP training at onboarding (for staff and third parties)
  - Ongoing education and periodic reminders
  - Periodic review and adjustment of employee awareness program aligned with evolving risks, threats, tools and technology
  - DLP exception and reporting process
  - Clearly defined behavioral expectations and consequences
  - Specific guidelines with Data Use Cases and examples to clarify expectations for functions or regions with unique requirements
Ensure Third Parties are Protecting Your Data

- Third-Parties – Vendors, Business Partners and other third parties play a critical role in protecting your critical and sensitive data
- Service Level Agreements - Clearly define data protection and breach notification requirements, and the consequences for failing to protect data
- Vendor Management Program - Include examination and reporting of required data protection, including self-assessments and site inspections
- Risk Management Program – Proactively work with vendors to identify and remediate risks, or choose alternate vendors….preferably before a breach occurs
Provide Incident Response for Data Breaches

• Data breaches can happen! An organization must be prepared

• Incorporate data breach response into your incident response procedures

• Key elements should include:
  – Reporting – Ensure employees know who to contact and what information to provide if/when a potential breach is discovered
  – Roles - Define an Incident Response Team (members, roles and responsibilities) with the appropriate knowledge to evaluate data breaches
  – Actions – Including notification, system shut down, recovery, data scrubbing, retention of data, chain of custody
  – Communications – Specific protocols for each stakeholder group, including internal, customer, shareholders, authorities, media
  – Breach Notification – Create predefined procedures for notifying affected parties, based on the different notification triggers
Select Supporting Tools and Technology

• Tools and technology need to be aligned with the goals and objectives of the DLP program

• DLP protection tool and technology options include:
  – Data discovery
  – Data fingerprinting
  – Access logging, monitoring and alerting
  – Encryption
  – DLP software and appliances (e.g., Content filtering)
  – E-mail content monitoring
  – Mobile device protection
  – Enhanced access controls
  – Firewalls, intrusion prevention, intrusion detection
  – Virus protection
  – Others…. 
Summary and Closing Remarks
Closing Observations

- Business and personal data will continue to be targets not only from external sources but internal as well
- Understanding your data is absolutely critical to protecting: what data is important, where your data is located, how it’s used, how your data flows during business transactions, etc.
- Threat profiles and business operations continuously change – implementing a strong risk management program to periodically re-examine DLP program effectiveness is important
- Effective DLP programs go beyond just implementing a tool
- Data breaches may still happen! Data breach notification and response plans are critical to minimizing business impact and regulatory fines
Summary and Closing Remarks

Primary Points of Contact

Debra Banning
Practice Leader, Information Security Center of Expertise
703-336-8169
debra.banning@experis.com

Steve Linker
Sales Director
403-605-7677
Stephen.linker@experis.com

Susan Chittick
Director, Risk Advisory Services, Canada
403-973-4730
Susan.chittick@experis.com