A holistic approach to data protection

Nev Zunic
IBM Distinguished Engineer, CTO, Global Data Security Services
1. Industry Trends and Current Environment
2. Data Categorization and Classification
3. Database Security
4. Endpoint Data Security – Encryption and DLP
5. Holistic Data Security
Industry Trends and Current Environment
Industry focus has evolved from the “T” to the “I” of IT
Security Challenges are Increasing in Number and Scope...

<table>
<thead>
<tr>
<th>EXTERNAL THREATS</th>
<th>INTERNAL THREATS</th>
<th>COMPLIANCE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sharp rise in external attacks from non-traditional sources</td>
<td>Administrative mistakes</td>
<td>National regulations</td>
</tr>
<tr>
<td>Cyber attack</td>
<td>Careless inside behavior</td>
<td>Industry standards</td>
</tr>
<tr>
<td>Organized crime</td>
<td>Internal breaches</td>
<td>Local mandates</td>
</tr>
<tr>
<td>Corporate espionage</td>
<td>Disgruntled employees actions</td>
<td></td>
</tr>
<tr>
<td>Government-sponsored attacks</td>
<td>Mix of private / corporate data</td>
<td></td>
</tr>
<tr>
<td>Social engineering</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

EXTERNAL THREATS
- Cyber attack
- Organized crime
- Corporate espionage
- Government-sponsored attacks
- Social engineering

INTERNAL THREATS
- Administrative mistakes
- Careless inside behavior
- Internal breaches
- Disgruntled employees actions
- Mix of private / corporate data

COMPLIANCE
- National regulations
- Industry standards
- Local mandates
A comprehensive data security solution needs to address all potential sources of data loss

<table>
<thead>
<tr>
<th>Source</th>
<th>Potential for breach</th>
</tr>
</thead>
<tbody>
<tr>
<td>Third-party partners</td>
<td>Confidential or corporate customer data may be lost or put at increased risk of exposure when transferred to a third-party.</td>
</tr>
<tr>
<td>Hackers</td>
<td>Consistent breach potential as hackers recognize that there is value to an organization’s data stores and will seek ways to compromise its security.</td>
</tr>
<tr>
<td>Mobile Devices</td>
<td>The movement toward improving productivity by empowering employees with more mobile devices and sharing of data has elevated the risk of potential data leakage</td>
</tr>
<tr>
<td>Social Networks</td>
<td>Increasingly used for corporate marketing purposes, social networks can present unforeseen risks in data leakage and damage to the brand</td>
</tr>
<tr>
<td>Employees</td>
<td>A significant amount of data leakage results from misuse by internal users, both intentionally and accidentally. 59 percent of individuals who were laid off, fired or quit their jobs in the past 12 months have admitted to stealing company data.</td>
</tr>
</tbody>
</table>

All Sensitive Data theft is now local and profitable ...

Cost of Global CyberCrime $388B

Global Black Market on Drugs $288B

http://www.symantec.com/about/news/release/article.jsp?prid=20110907_02
Data management issues organizations are facing

Do you know what your data & information assets are? Do you know where your data came from? Do you know what has happened to it?

Who owns the data?
Who can modify or delete the data?
Who can use the data?
Who should?

Where should data be kept? Should it be safeguarded?

Do you know the value of your data and economic risk of loss?

How do you address both data consolidation and data aggregation requirements?

How do you demonstrate compliance with data centric regulations?

How long do you need to keep your data?

Platform infrastructure ↔ Lifecycle ↔ Trusted Information ↔ Protection ↔ Extended enterprise

Do you know what your data & information assets are? Do you know where your data came from? Do you know what has happened to it?

Who owns the data?
Who can modify or delete the data?
Who can use the data?
Who should?

Where should data be kept? Should it be safeguarded?

Do you know the value of your data and economic risk of loss?

How do you address both data consolidation and data aggregation requirements?

How do you demonstrate compliance with data centric regulations?

How long do you need to keep your data?

Platform infrastructure ↔ Lifecycle ↔ Trusted Information ↔ Protection ↔ Extended enterprise

Do you know what your data & information assets are? Do you know where your data came from? Do you know what has happened to it?

Who owns the data?
Who can modify or delete the data?
Who can use the data?
Who should?

Where should data be kept? Should it be safeguarded?

Do you know the value of your data and economic risk of loss?

How do you address both data consolidation and data aggregation requirements?

How do you demonstrate compliance with data centric regulations?

How long do you need to keep your data?

Platform infrastructure ↔ Lifecycle ↔ Trusted Information ↔ Protection ↔ Extended enterprise

Do you know what your data & information assets are? Do you know where your data came from? Do you know what has happened to it?

Who owns the data?
Who can modify or delete the data?
Who can use the data?
Who should?

Where should data be kept? Should it be safeguarded?

Do you know the value of your data and economic risk of loss?

How do you address both data consolidation and data aggregation requirements?

How do you demonstrate compliance with data centric regulations?

How long do you need to keep your data?

Platform infrastructure ↔ Lifecycle ↔ Trusted Information ↔ Protection ↔ Extended enterprise
Data Security Challenges

Highlights from Verizon 2012 Data Breach Investigations Report

- In 2011, 855 incidents reported
- 174 million compromised records
- Lack of Appropriate Controls

- 98% of data breaches stemmed from external agents.
- 97% of data breaches were avoidable through simple or intermediate controls.
- 96% of victims were not PCI DSS-compliant at the time of the breach.
- 96% of breaches involved database servers representing an 18% increase from 2010. – 98% in Enterprises over 1000 employees
- 92% of victims were notified by 3rd parties of the breach. – 49% of organizations over 1000 employees
- 85% of victims were unaware of the compromise for weeks to months.

Source: 2012 Verizon Data Breach Investigations Report
Compromises take days or more to discover in 96% of cases; and weeks or more to contain in over 91% of cases.

<table>
<thead>
<tr>
<th>Time Span of Events by Percent of Breaches</th>
<th>Seconds</th>
<th>Minutes</th>
<th>Hours</th>
<th>Days</th>
<th>Weeks</th>
<th>Months</th>
<th>Years</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initial Attack to Initial Compromise</td>
<td>10%</td>
<td>75%</td>
<td>12%</td>
<td>2%</td>
<td>0%</td>
<td>1%</td>
<td>0%</td>
</tr>
<tr>
<td>Initial Compromise to Data Exfiltration</td>
<td>8%</td>
<td>38%</td>
<td>14%</td>
<td>25%</td>
<td>8%</td>
<td>8%</td>
<td>0%</td>
</tr>
<tr>
<td>Initial Compromise to Discovery</td>
<td>0%</td>
<td>0%</td>
<td>2%</td>
<td>13%</td>
<td>29%</td>
<td>54%+</td>
<td>2%</td>
</tr>
<tr>
<td>Discovery to Containment/Restoration</td>
<td>0%</td>
<td>1%</td>
<td>9%</td>
<td>32%</td>
<td>38%</td>
<td>17%</td>
<td>4%</td>
</tr>
</tbody>
</table>
Security is “Reactive” – needs to become “Pro-Active”

Data is a Corporate Asset

**Reactive**

*Think like a defender, defense-in-depth mindset*

- Emphasize the perimeter
- Patch systems
- Use signature-based detection
- Collect logs

**Pro-Active**

*Think like an attacker, counter intelligence mindset*

- Identify and Protect high value Data
- Emphasize the data
- Apply Appropriate Controls
- Align Data Security with Business Objectives
Data Categorization and Classification
Getting started with Data Security

• A comprehensive data security program entails the following:
  – Sensitive data discovery
    • Structured data
    • Unstructured data
  – Data taxonomy and classification
    • According to business processes
  – Database security reference architecture and assessment
    • Provides prescriptive guidance on security controls
  – Data Loss Prevention
    • Within network and at endpoints
  – Endpoint encryption
    • Protect sensitive assets due to loss of devices
  – Data masking
    • Protect sensitive information assets in development and test environment
### Organizations Need a Comprehensive Enterprise-wide Approach to Data Security and Compliance

<table>
<thead>
<tr>
<th>Understand and define sensitive data</th>
<th>Assess vulnerabilities</th>
<th>Monitor database activity</th>
<th>Help protect sensitive data</th>
<th>Manage access</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Capabilities:</strong></td>
<td><strong>Capabilities:</strong></td>
<td><strong>Capabilities:</strong></td>
<td><strong>Capabilities:</strong></td>
<td><strong>Capabilities:</strong></td>
</tr>
<tr>
<td>✓ Discover database instances</td>
<td>✓ Automated database</td>
<td>✓ Continuous, real-time</td>
<td>✓ Mask information using</td>
<td>✓ Centralize and</td>
</tr>
<tr>
<td>✓ Automate detection of sensitive</td>
<td>vulnerability assessment and remediation suggestions</td>
<td>database activity monitoring</td>
<td>realistic values</td>
<td>automate collection of entitlement information</td>
</tr>
<tr>
<td>data in databases</td>
<td>✓ Audit any configuration or security setting changes</td>
<td>✓ Comprehensive audit trail</td>
<td>✓ Automate key management process</td>
<td>✓ Assess privileges granted directly and indirectly</td>
</tr>
<tr>
<td>✓ Automate responsive actions</td>
<td>✓ Discover sensitive data in documents</td>
<td>✓ Policy-based controls to detect unauthorized or suspicious activity</td>
<td>✓ Database encryption</td>
<td>✓</td>
</tr>
<tr>
<td>✓ Discover sensitive data in</td>
<td>✓ Create a data taxonomy</td>
<td>✓ Review and update policies and procedures</td>
<td>✓ Redact data in documents and forms</td>
<td>✓</td>
</tr>
<tr>
<td>documents</td>
<td>✓ Classify sensitive data</td>
<td></td>
<td>✓ Endpoint and network data loss prevention</td>
<td>✓</td>
</tr>
</tbody>
</table>

**Create a DBMS Security Reference Architecture and Governance Framework**
Data Needs to be Managed Throughout its Lifecycle

- Valuation: What is the data worth to the enterprise?
- Protection: Is the data privacy and security assured?
- Insights: Have we extracted the value in both public and private data?
- Sharing: Are the right people able to use it?
- Managing & Monitoring: Can we manage it as it moves throughout the enterprise? Are we audit ready and compliant?
- Storage: Is it properly stored and backed up?
- Deletion: Is it systematically deleted at the end of its useful life?
- Acquisition & Discovery: Where are the data in the enterprise or elsewhere?
- Cleanse & Load: Prepare the data for analysis

Cleanse & Load

Acquisition & Discovery

Valuation

Protection

Insights

Sharing

Managing & Monitoring

Storage

Deletion
A Data-Centric Maturity Model

1. We protect our structured data, don’t we?
2. We use best practices in protecting our data
3. We actually know where all of our data is
4. We have protected our data in proportion to its value
5. We even know where our valuable data is when it’s in motion
6. We’ll get to our unstructured data later
7. We’ve got whole-disk encryption for laptops
8. We’ve figured out which data is valuable
9. We’ve protected our most valuable data
10. Our data’s protected even for Mobile

Structured Data

Unstructured Data (Text, Images)

Maturity

Time
An approach to classifying enterprise information assets

A four-pronged approach is recommended to discover and classify information assets within the enterprise:

- **Activity 1**: Reach organizational consensus on which data are most valuable to the business
  - Establish taxonomy of data categories for the business
  - Interview key stakeholders and determine the value of different categories of data
  - Rank-order the categories by value
  - Estimate relative value of categories

- **Activity 2**: Categorize existing information
  - Estimate value of structured data
  - Estimate value of unstructured data

- **Activity 3**: Determine high-value data protection (relative to its value)

- **Activity 4**: Classify new information at a granular level
  - Use automated classification systems to classify data
  - Classify data as it moves (e.g., to Mobile devices)
Data Classification Challenges

- Gaining consensus on sensitivity ranking and value of data
- Gaining consensus on data taxonomy
- Developing standards on how the sensitive data assets should be protected
- Developing plans and gaining support to improve protection levels
- Assigning owners to information categories
- Identifying entities with access privileges and determining appropriateness of access
- Establishing an ongoing business process for classification
- Determining whether controls are in compliance with requirements
- ...and more
Database Security
End-to-end data protection begins with understanding the types, sources, and value of a company’s information assets

• An organization’s most sensitive information assets reside in database management systems

• The information assets are vital to ongoing business operations, business sustainability, and demonstrating compliance to regulatory requirements as well as industry standards

• The threats and exposures to these sensitive assets are getting more sophisticated and increasing on a daily basis

• Applying proper protection measures to database systems is an absolute necessity in today’s interconnected world in order to mitigate risks, deter attacks, and comply with requirements

A database assessment needs to be inclusive of people, processes, and procedures

Enterprises must begin developing and implementing best practices for data security breach disclosure and notification. This critical imperative is being driven fundamentally not only by regulatory requirements for disclosure, but also by the growing recognition that failure to do so is bad for business. – Gartner, 2010

• Average cost of a data breach incident is $6.7 million ($204 per compromised record)
• FDIC may levy fines from $5,000 to $1,000,000 per day
• GLB sections 501 & 503 enable criminal penalties (Ponemon Institute, ’09)
Database servers are the primary source of breached data

$5.5 Million

The average total cost per reporting company is $194 per record or US$5.5 million per breach.

Sources: Ponemon Data Breach Study - 2012

"Establishing a strategy for database security is no longer optional"

Published: 29 November 2011, Gartner report

"Information is itself the target. Information is the world’s new currency."

— Ralph Basham, Director, United States Secret Service

Although much angst and security funding is given to offline data, mobile devices, and end-user systems, these assets are simply not a major point of compromise.

Why?

- Database servers contain valuable information assets
  - Financial records
  - Credit card and other account records
  - Patient records
  - Personally identifiable information
  - Customer data
- High volumes of data
- Structured for easy access

“Information is itself the target. Information is the world’s new currency.”

— Ralph Basham, Director, United States Secret Service
In 2011, there was a rise in the number of significant breaches reported by organizations presumed operationally competent.

Risks are increasing:

- Attacks are getting more sophisticated
- Advancement and adoption of newer technologies/computing paradigms such as mobile devices, social networks, and cloud
- Poor design, implementation and maintenance (e.g. Database Management, Application Testing)
- Underinvestment in legacy infrastructures is exposing enterprises
Sampling of security incidents in 2012

Source: IBM X-Force® Research and Development
Many exposures and exploits exist due to a lack of robust DBMS processes and procedures

DBMS processes & procedures present numerous avenues for introducing potential exposures, inclusive of:

- Change Management
- Privileged Access Control
- Data Inventory
- Encryption
- Patch Management
- Configuration Management
- Vulnerability Management and Testing
- Data Governance
- Monitoring
- Metrics
- Security Guidelines and Controls
- Enterprise Security Architecture
- Auditing
- Systems Delivery Lifecycle
- Solution Patterns
- User Provisioning
- De-provisioning process
- Protect Confidential Information
- Use of Production data in non-production environment
- Separation of duties conflicts

...and, the lack of a robust architecture and modeling tool may inadvertently (or purposely) introduce points of vulnerability and exposure
DB Management & Security Governance Framework and Reference Architecture

**Business and Corporate Strategy**
- Business and Management Objectives
- Set the vision and requirements

**Standards and Policies**
- DB Policies
- Legislative and Compliance Requirements

**DB Governance**
- DB Management and Governance Controls
- DB Management and Security Governance Focus Areas

**Empowers**

** Enables & enhances**

**DB Management and Security Reference Architecture**

**Capabilities**
- Compliance
- Best Practices
- Communication
- Stakeholder Accountability
- Implementation Guidelines

**Enables & enhances**

**Empowers**

**SymanTEC VISION 2013**
DBMS Management and Security Architecture Topics

- Identity management – authentication, authorization strategy
- User provisioning
- Data discovery
- Data classification
- Encryption
- Audit
- Monitoring
- Access control
- Change management
- Patch management
- Testing
- Vulnerability scanning
DB Management and Security Architecture Model

Refine & Align

DB Planning & Management
- Business Requirements
- Business & IT Processes
- Regulatory Requirements

Configures

Acquisition

Architecture Investment

Normalizes

Security Policy

Defines

DB Security
- Business Case
- Change Management
- Internal Controls
- Patch Management
- Configuration Management
- SDLC

Testing & Certification

Access Rules

DB Design
- DB Compliance
- DB Architecture
- Security Model
- Access Rules

DB Compliance

DB Engineering
- Capacity Mgmt.
- Versioning
- Monitoring, Reporting

DB Modeling
- Data Ownership
- Data Classification

Approved and Maintains

Confidential Information Management
- Data Discovery & Inventory
- Data Encryption
- Data Masking

Internal Controls
- Metrics
- Monitoring
- Database Auditing

Normalization

Validation, Reporting & Awareness

RBAC

Data Labeling:
- Owner
- Type of Data
- Sensitivity
- Retention Period

Monitoring, Reporting & Awareness

Drives

SDLC

Enforcement

User Provisioning
- Authentication Authorization Privileged Access Control

Access Control

Normalizes

Translation

Configures

Vulnerability Management

Testing & Certification

Change Management

Patch Management

Configuration Management

SDLC
Complement secure databases with endpoint security

Most of the front end security layer protection cannot stop all the threat vectors.

→ Need the last layer of protection at the data level.
Data Loss Prevention (DLP)

Symantec Data Loss Prevention software is a comprehensive, content-aware solution that discovers, monitors, and protects confidential data wherever it is stored or used – across network, storage and endpoint systems.

Key Features

- **Discover**—Find confidential data wherever it is stored, create an inventory of sensitive data, and automatically manage data cleanup.
- **Monitor**—Understand how confidential data is being used whether the user is on or off the corporate network, and gain enterprise visibility.
- **Protect**—Automatically enforce security policies to proactively secure data and prevent confidential data from leaving an organization.
- **Manage**—Define universal policies across the enterprise, remediate and report on incidents, and detect content accurately within one unified platform.

Key Benefits

- Reduce proliferation of confidential data across enterprise data centers, client systems, remote offices, and end-user machines.
- Identify broken business processes transmitting confidential data.
- Monitor and protect communications of sensitive content to public websites.
- Define and deploy universal policies across the enterprise.
The type of encryption solution needed is determined by use cases

For example, with encryption solutions, you can...

<table>
<thead>
<tr>
<th>Enhance protection of stored data even when an endpoint device is lost or stolen</th>
<th>Using ...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protect data more effectively while it’s in use on an endpoint device</td>
<td>PGP Whole disk encryption (WDE)</td>
</tr>
<tr>
<td>Monitor and control the use of external storage devices for storing and transporting data</td>
<td>Encryption of files, folders, virtual disks (VDisks) and shared media</td>
</tr>
<tr>
<td>Enhance the security of inbound and outbound e-mail</td>
<td>Symantec Endpoint Encryption</td>
</tr>
<tr>
<td></td>
<td>PGP email encryption and digital signing</td>
</tr>
</tbody>
</table>
Endpoint Data Security – Encryption and DLP
End user devices are another source of data loss, especially for confidential business data and intellectual property

Travelers Left Behind More Than 8,000 Mobile Devices at Top U.S. Airports

Credant Technologies, the trusted expert in data protection, today announced the results of their second survey of top airports in the United States. In the last year, travelers left behind **8,016 mobile devices** at seven of the largest airports in the country, including: Chicago O’Hare, Denver International, San Francisco International, Charlotte Douglas, Miami International, Orlando International and Minneapolis/St. Paul.

Additionally, there is an increasing focus on protecting intellectual property

- Apple becomes world’s biggest Mobile Technology Litigation Company in last two years
- 2011 is a year of tech and publishing lawsuits, by the numbers
- Breach of IP is not regulated and therefore not often heard on the news

“The U.S. economy relies heavily on intellectual property; virtually every industry either produces IP or uses it.”

Endpoint Data Protection - Products at a Glance

**SEE Device Control**
- Granular device control with whitelisting ensures authorized use of removable devices and ports

**Symantec Drive Encryption**
- Full disk encryption for desktops, laptops, and Windows® servers.
- Supports Windows®, Mac OS®, and Linux® platforms

**SEE Removable Storage Edition**
- Software-based and self-contained encryption on any USB device or optical media
Symantec File and Server Protection – At a Glance

Symantec File Share Encryption: Shared File Protection
- Protect data exchanged between users via shared network folders
- Encrypt files stored in the cloud

File Share Encryption for iOS
- Access File Share encrypted files from the cloud on your iPad

FILE AND SERVER ENCRYPTION

PGP® Command Line: Scriptable Encryption
- Integrate encryption into data transfer, data distribution and data backup processes
Let’s start by answering these questions about the data

• Where did the data originate?
• Who owns the data?
  Who or what can modify the data?
  Who or what can delete the data?
• What type of data is it?
  How sensitive is the data??
• Who or what can use the data?
  For what purpose?
  Can it be shared?

• Where will the data be kept?
• Does it need to be safeguarded?
  At rest?
  During transmission?
  During use?
• How long do we need to keep the data?

A data security architecture that ties together all the information control components is critical to the survival of global firms
Data Centric Security

Data centric security architecture is a **dynamic and adaptable control system** that enables compliance with new corporate and legislative requirements without having to re-configure the IT environment.
Data Centric Security Architecture (DSCA)

An architectural model that places emphasis on critical assets in complying with legal and regulatory requirements while empowering the user to perform their job responsibilities.
Policy-Based Data-Centric Architecture

Static Verification
- Business Process System
  - Business Process Logic
  - Application Logic
- Policy Engine
  - Verifiable Model
  - Access Rule
- Security Policies
  - Security Model
  - Data Classification Model

Policy Mapping
- Business Regulations
- Business Processes

Dynamic Control
- Users
  - authenticates
- Organization Directory
  - requests data and responses
  - authenticates
- Authentication
- Access Enforcement
  - requests data and responses
  - authenticates
- Role
- Usage Log
  - classifies
  - Static Verification
  - statically verifies
  - statically verifies
  - statically verifies
  - verifies
  - verifies
  - verifies
  - defines
  - normalizes
  - normalizes
  - normalizes
  - implements
  - implements
  - implements
  - implements

Data Elements
- Label:
  - Owner
  - Type of data
  - Sensitivity of data
  - Retention period

Requirements
- Business Processes
- Business Regulations
Test Data: The Easiest Way to Expose Sensitive Data

Test data stored on portable devices, such as laptops or memory devices.

**April 2008:** The theft of a laptop in New York contained the data on over 170,000 people who had used the services of a blood bank.

Test data sent to and used by third-party consultants and overseas partners/teams.

**October 2008:** An IT contractor for a large American oil company used personnel data as part of an unemployment insurance claims scam.

Confidential data available to and viewed by developers, testers and trainees.

**March 2008:** The State Department reported the unauthorized access of [then] Senator Hilary Clinton’s passport information. The breach was traced to a training seminar.
Thank you!

- Nev Zunic
- zunic@us.ibm.com
- 845-264-8384