

Information Security Incident Management

Operationalizing Your Incident Response Plan

As data breach events headline national newspapers with greater frequency, organizations are searching for a systematic approach to the collection and identification of potential incidents that may involve a breach of confidential information. Whether this confidential information encompasses strategic information or Personally Identifiable Information (PII) involving employee, customer, or consumer data, the impact of an information security breach creates significant risk and exposure to the organization.

Today, many organizations are implementing policies and procedures for information loss and are spending hundreds of thousands of dollars on data protection and information security solutions. However, no matter what policies, procedures, and prevention systems are in place, organizations will continue to experience loss of confidential information in the dynamic “information age” that drives businesses today.

Working with privacy practitioners, EthicsPoint has developed an information security incident management tool that helps operationalize incident response planning and bridge the gap between data loss preventions and breach notification procedures. As a leading incident management solutions provider in the Governance, Risk, and Compliance (GRC) market, EthicsPoint has expanded its process and workflow management tool to assist organizations with:

- *Identification of potential confidential information security breaches*
- *Preliminary screening and risk assessment*
- *Investigative and task management*
- *Collaboration with internal and external stakeholders*
- *Breach response plan management*
- *Affected-party notification process*
- *On-demand management reports*

This tool represents a focused practice layer of EthicsPoint’s Issue and Event Manager™ solution. This solution provides a single system for capturing, managing, and resolving a wide variety of incidents across a broad range of functions, including:

- *Flexible, client-defined configuration that tailors the solution to each organization*
- *Client-defined roles and/or skill-based access levels and privileges*
- *Incident intake from, and interface with, a variety of sources and applications*
- *Sophisticated administrative features that allow for easy management of users*
- *Workflow automation and process control that allows for consistent, complete follow-up of all cases*
- *End-to-end network and data security to ensure redundancy, scalability, and reliability*

For More Information

To learn more about EthicsPoint
www.ethicspoint.com | 866.297.0244 | sales@ethicspoint.com

©2008 EthicsPoint, Inc. All Rights Reserved Jun 08

COST OF DATA BREACH

*Data breaches continue to become more expensive: Costs to companies weigh in at a hefty average of **\$202 per compromised record**. That’s a 2.5% increase over the 2007 average cost of \$197. Other notable findings: Average data breach cost per incident: \$6.6 million.*

- Source: Ponemon Institute’s “2008 Cost of Data Breach Study”; Available from the Ponemon website: <http://bit.ly/crrbK>

INCIDENT COLLABORATION (INTERNAL STAKEHOLDER):

- *Legal (General Counsel)*
- *Business Unit Leaders*
- *Corporate & IT Security*
- *Human Resources*
- *Risk Management*
- *Corporate Communications*

INCIDENT COLLABORATION (EXTERNAL STAKEHOLDERS):

- *Outside Counsel*
- *Investigative Firm*
- *Forensics Firm*
- *Law Enforcement Agencies*
- *Third-Party Notification Services*

INFORMATION BREACH TYPES:

- *Employees*
- *Customers*
- *Consumers*
- *Intellectual Property*
- *Confidential Business Documents*



Ethics Hotline

Departmental Identification

Privacy Hotline

Security Detection Systems

POTENTIAL INCIDENT IDENTIFICATION

INCIDENT SCREENING

HRIS Lookup (Originator): - Title - Department	Incident Type	Screening Questionnaire: <i>(Questions that help identify the probability of a security breach)</i>
Location Database Lookup	Data Storage Medium	

INCIDENT RESPONSE ACTIVITIES

Internal Department Notifications: - Legal - Business Unit - Corporate and IT Security - Ethics and Compliance - HR - Risk Management - Corporate Communications	Incident Case Management: - Stage of Investigation - Confidential Information Inventory - Policy and Procedure Violation - Roles- and Skills-Based Access Levels - Documentation Repository - Complete Audit Trail - Disposition of Loss Originator
--	---

INVESTIGATIVE COLLABORATION & TASK MANAGEMENT

Internal Collaboration: - Loss Originator/Management - Legal - Business Unit - Corporate and IT Security - Ethics and Compliance - HR - Risk Management - Corporate Communications	External Collaboration: - Outside Counsel - Investigative Firm - Forensics Firm - Law Enforcement Agencies - Federal - State - Local (County, City)
---	---

BREACH DETERMINATION & RESPONSE PLAN

BREACH RESPONSE MANAGEMENT

Breach Response Program Types: - Employee Records - Customer and Consumer Data - Business Confidential	Breach Response Plan (Third Party): - Affected Party Files - Response by State - Approved Documentation
--	---

NOTIFICATION MANAGEMENT

Affected Party Notification Mailing → Call Center Support → 12-Month Credit Monitoring Service → Tri-Merge Credit Report → Investigation and Restorative Services

TRANSPARENCY/MANAGEMENT REPORTS

Third-Party Breach Notification Service Provider