MANAGING TECHNOLOGY: DATA IDENTIFICATION & CLASSIFICATION

GTC East - Albany, NY
September 24, 2009

Deborah Snyder, CISSP, GSLC, PMP
Chief Information Security Officer
NYS Office of Temporary Disability Assistance

Slawomir Marcinkowski, CISSP
Information Security Consultant
NYSTEC

WHAT'S ALL THE FUSS ABOUT?

IT'S JUST DATA…

RIGHT?

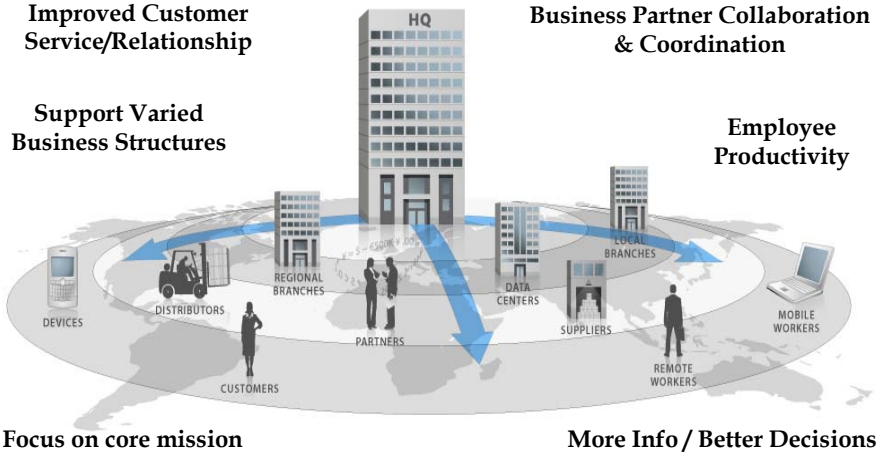
Our Service Models Have Changed…

Improved Customer Service/Relationship

Business Partner Collaboration & Coordination

Support Varied Business Structures

Employee Productivity



Focus on core mission

More Info / Better Decisions

…Bringing New Risk Management & Information Security Challenges…

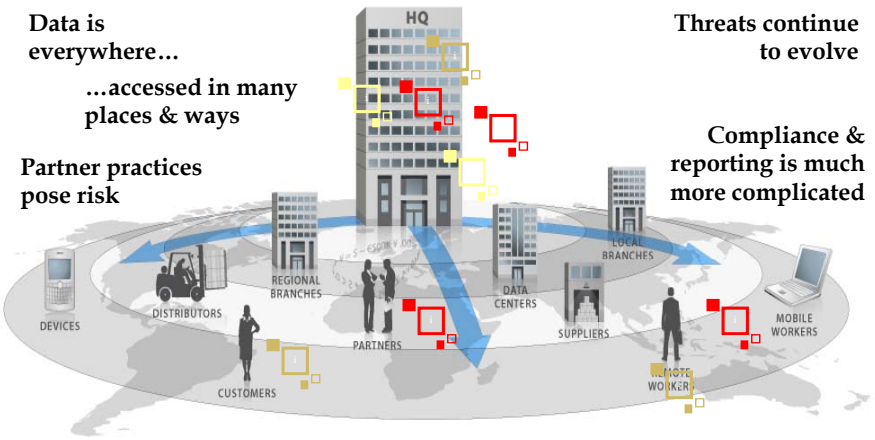
Data is everywhere…

…accessed in many places & ways

Threats continue to evolve

Partner practices pose risk

Compliance & reporting is much more complicated



So, what's an agency to do?

- You can't protect against all threats…
- Need a "Divide & Conquer" strategy…
  - Some information assets require more protection than others.
  - Protection measures must be "right -sized" - appropriate to the asset being protected.
- Classification is the key to selecting the right controls to assure adequate protection!

How/where does one begin?!?

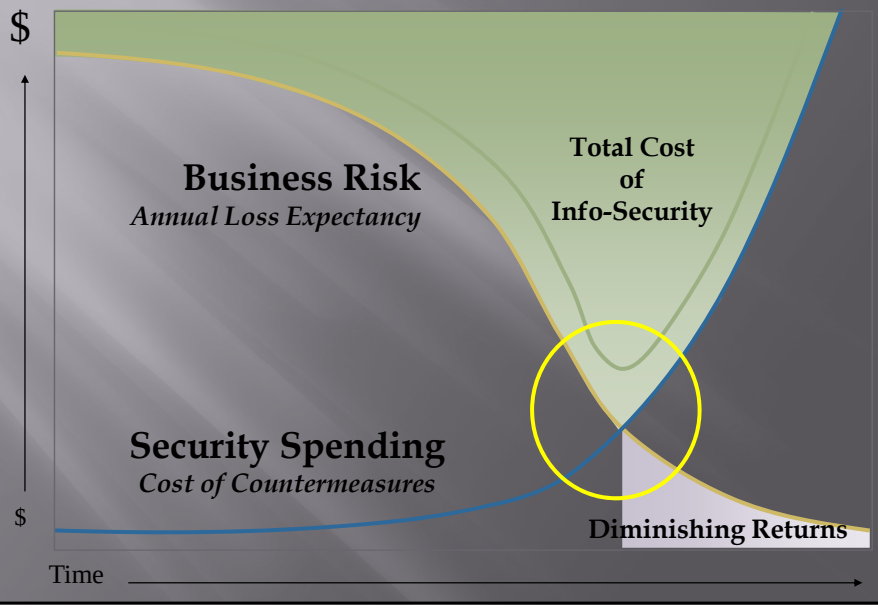
- Risk management framework
  - Assets should be prioritized based on value
  - Loss expectancy is driven by "likelihood "of loss
  - Countermeasure cost should be appropriate for risk exposure & loss expectancy

- Information Classification
  - Direct & indirect loss aspects.
  - Roles & responsibilities for data protection.
  - Rules of engagement if an incident occurs.

It's amazing how many businesses take this approach to understanding & addressing RISK!

The ostrich does many things, but hiding its head in the sand is actually not one of them. (*digitally constructed image)

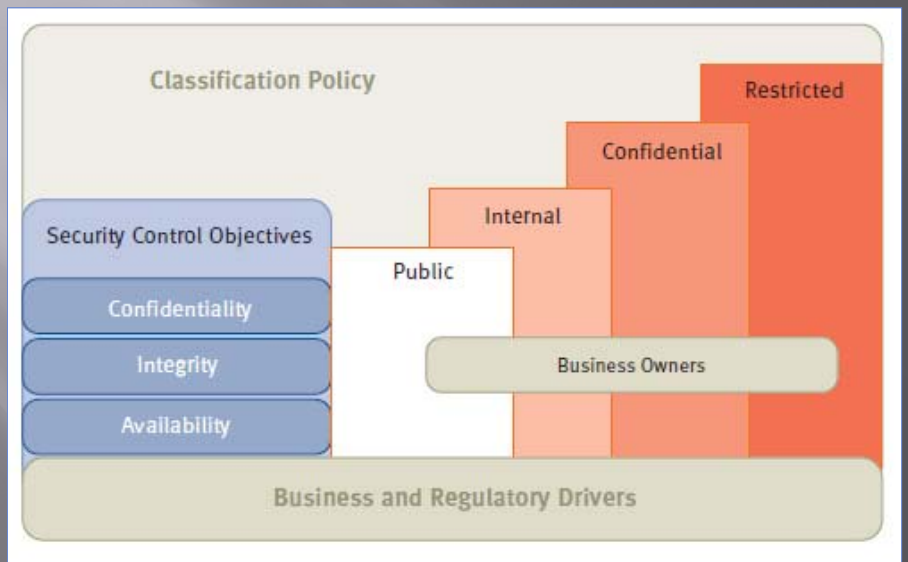
Risk Management Approach



Risk Management Framework

- Information Security Assurance requires a risk-based approach…
- Classification is a vital data protection 1st step.
- Data is classified based on "Sensitivity & Criticality" (to the business)…
- Identify threats & potential impact (risk)…
- Select & implement controls to mitigate risk to acceptable level.

"View From The Top"



Source: RSA, Security Division of EMC, **Classification for Information Security -** Securing data according to business risk

High-Level Process

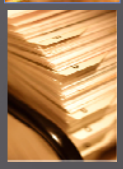
Quickly classifying according to risk level is an important step in identifying business critical systems/data & prioritizing security controls.

Inventory

- Portfolio profiling quickly classifies data/systems according to their associated risk level

Classification

- Identification of most critical information assets
- Based on criticality, sensitivity or compliance needs
- High-level assessment of information security impact:
  - Defines data, application/system controls & functions
  - Data / system criticality
  - Data / system sensitivity



Impact Assessment

- Impact assessment based on NIST SP800-30
- Qualitative risk assessment
  - Attributes a subjective value to risk when reliable data on likelihood & costs are not available
  - Depends more on expertise, experience & judgment of the assessors
- Rate potential damage based on:
  - Asset criticality assessment (e.g., impairment of business function, financial loss)
  - Data criticality & data classification
  - Data sensitivity (e.g., exposure of PII)

Consider Direct & Indirect Costs

- Direct costs
  - Fines and penalties
  - Disclosure and follow up
  - System and staff resource costs for remediation
- Indirect costs
  - External oversight and coordination
  - Testimony and Public Relations
  - Civil litigation – maybe even years later

Loss Expectations

- Assets & resources have an intrinsic value
  - Single laptop device may be worth $2,000
- Assets & resources also have a strategic value
  - The sensitive information on a single laptop device could potentially be worth millions (&/or cost millions in mitigation & notification expenses)

Balance Security with Business Needs

- Controls protect information based on a determined classification level
- Review controls with BU
  - Controls baseline
- When controls compete
  - Flexibility is key… assess risk
  - Develop compensating controls
  - Understand & document residual risk

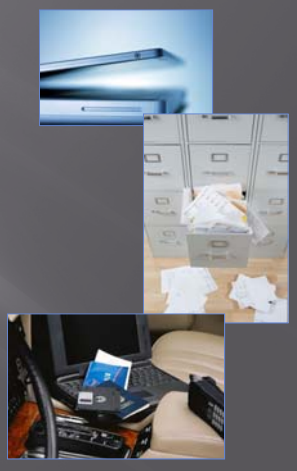
14

Scenario

- A $2,000 laptop containing 100,000 confidential, personal private or sensitive records is lost/stolen…
  - Property loss impact - $2,000
  - Minimum cost to mitigate event ~ $10,000,000+ (industry estimate of minimum mitigation cost of $100/lost identity)
  - Operational cost of disclosure mailing ~ $75,000 (assumes $0.75 per person to print & mail a disclosure letter)
  - Impact on agency funding & additional regulatory oversight (potential lost funding, penalties, additional audits)
  - Reputational Impact - bad publicity, public perception, impact on agency operations

Also consider…

- Is the situation any different if the laptop never left the building, but the data did?
- Is the situation any different if the data were on a PDA, magnet tape, DVD or other forms of portable device or media?
- Is the situation any different if the data were on paper, rather than in electronic form?



Key Points

- It's really not a technology issue at all...
- It's a risk management driven business concern…
- Information Classification gives you a ***clear road map*** for your information risk management & data protection efforts!
- Quite simply, it's just part of doing business!

From the Trenches

"Key Success Factors & Pitfalls"

Key Success Factors

- Risk Management-based Framework
- Executive Commitment/Sponsorship
- Business-led Effort
- Data Classification Standard - well-defined methodology
- Consider Data in all Forms/Life Cycle Phases
- Planned/Managed Initiative
- Cross-Sectional Team
- Phased-in Approach
- Education & Communication
- Classify by Data Type/Category

Terms of Engagement

- Executive Commitment/Sponsorship
- Business-led Effort - Information Owner
- Cross-Sectional Team
- Education
- Communication

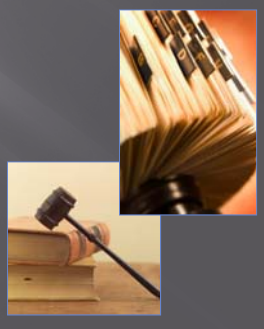
Executive Management Buy-in

- Data Classification must be sanctioned by the highest levels in your organization
- How did we achieve
  - Understand data produced &/or handled by your agency
  - Link to current business initiatives
  - List benefits
  - Link to regulatory drivers

21

Regulatory Drivers

- **FISMA**
  - Federal Information Security Management Act
  - Federal agencies & subcontractors (State grantee agencies) are obliged to conform
  - Requires use of NIST data classification standard
- **Special Regulations**
  - Internal Revenue Service
  - Social Security Administration
  - HIPAA
- **Contracts**
- **Intergovernmental MOUs**
- **Court Orders**



Planning & Management

- Planned/Managed Initiative
- Phased-in Approach
- Defined Roles & Responsibilities
- 3rd Party Responsibilities

Find a Committed Business Unit

- Start with a prototype…
- Identify a Business Unit (BU) in your organization where they will get the most benefit.

- Convey that it will be a collaborative effort
- Will require assigned resources
- Understand there will be unexpected obstacles & delays

24

Execute an MOU

- Memorandum of Understanding (MOU)
  - Establishes a framework with the Business Unit (BU) and the Data Classification team to work together to classify and secure the BU's information.
  - Identifies the process and associated roles and responsibilities of each party as they relate to the classification and security of the BU.
    - Information owners
    - Data Classification team
    - Consultants
- Senior Executive Sign Off

25

Manage the Business Partnership

- MOU guides the process
- Defines mutual expectations
- Clarifies roles and responsibilities
- Plan of action
- Time frame
- Resource Commitment
  - Data Classification Team
- Formal periodic updates

26

Include in Scope…

- Information Assets Inventory
- Data in all forms/life cycle phases
- NYSARA & FOIL requirements
- Merged data
- Meta data
- Reproductions
- 3rd Party data

Who makes the decision?

- Information Owner - the business unit /program area that "owns" the data

- Executive Policy-Makers
- Legal Counsel
- FOIL Officer
- Business Analysts
- Information Security Officer
- Information Custodians

Data Classification Team

- Leads the actual data classification process
- Choose team members with an understanding of your business processes and data used in these processes

- Classification can be subjective…
- Best done as a collaborative task that considers:
  - Business
  - Technical
  - Knowledge, Learning, Environmental

29

Data Classification Methodology

- Well-defined Data Classification Standard
  - Classification Scheme
  - Procedures
  - Baseline Controls

- Classify data by type/category
- Templates, tools & techniques

Data Classification Schema – What's it based on?

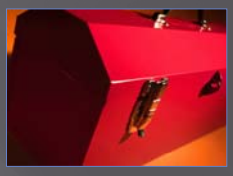
Data Class (Confidentiality, Integrity, Availability)

RISK ASSESSMENT: **High-Low** **High-Low** **High-Low**

- **NIST**
  - Confidentiality (i.e. Risk of disclosure)
  - Integrity (i.e. Risk of data corruption)
  - Availability (i.e. Risk of not granting access)
- **NYS Data Classification Standard**

Data Classification Toolkit

- Used by Data Classification Team
- Asset Inventory Sheet (pre work)
  - Records information about the information asset
    - Source, Purpose and Value of Asset
    - Legal Requirements
    - Retention and Disposition Requirements
    - Who the Information Users are
    - Impact on Agency (e.g. reputation, public trust)



- Electronic Repository
  - Information from Asset Inventory Sheet
  - Maintained for the organization

32

Data Classification Maintaining the "Process"

- Data Classification is an ongoing process…
  - Requires on going commitment from the organization
  - Need to assign responsibility within the organization
  - It cannot be considered static… it must be interwoven into the business process

33

Potential Pitfalls

- Biting off too much…
- Not documenting rationale…
- "Overclassification…"
- Failure to build classification in…
- Considering it done!

Questions

& hopefully, further dialog…

Deborah Snyder, CISSP, GSLC, PMP
Chief Information Security Officer
NYS Office of Temporary Disability Assistance
Deborah.Snyder@otda.state.ny.us

Slawomir Marcinkowski, CISSP
Information Security Consultant
NYSTEC
slaw@nystec.com

35