Cybersecurity Panel Discussion

NJ IMA Council
2016 Fall Conference
October 24, 2016

Deborah Butler, Esq.

Former Director, Knowledge Assurance, Dell

Key Take-Aways

- People are the weakest link in the controls process
- Technology is only a tool; use it to enable holistic information governance
- Data classification is foundation to information governance (not all data is created equal)
- Understand value and power of data classification (data privacy, data protection and data management – retention/disposition)
- Data protection is a journey…

➢ A journey that begins with understanding:

➢ Your company’s risk/tolerance and culture

Data Threats, By the Numbers

$3.5M

Average spend for companies to investigate, notify and respond to a data breach in 2014*

$300B

Annual cost/losses for U.S. companies due to corporate espionage including intellectual property theft*

46%

The percentage of IT security leaders whose companies have a common process in place to discover and classify on-premise confidential data*

- 1 in 5 Americans fell for online scams
- More than 50% lost money
- 50% of victims 18 – 34 years old

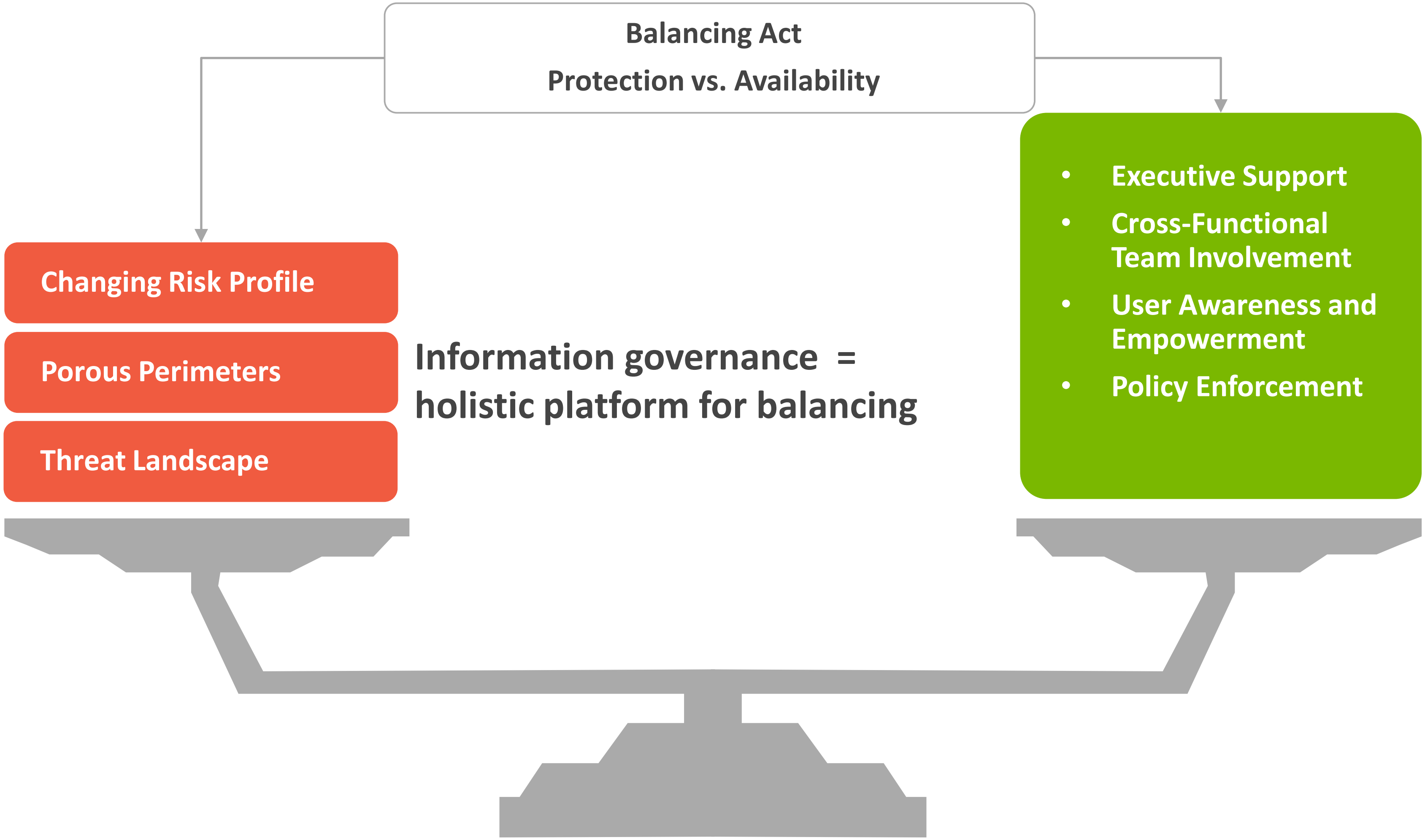
- 2016 Microsoft Study

1. Source: “2014 Cost of Data Breach Study: Global Analysis” by Ponemon Institute, May 2014.

2. Source: “Cybercom Chief Details Cyberspace Defense,” American Forces Press Service, September 23, 2010. Later re-quoted in the IP Commission’s “Report on the Theft of American Intellectual Property.”

3. Source: “The State of Data Security Intelligence” by Ponemon Institute, April 2015.

The Age-Old Challenge of Protection vs. Availability



Balancing Act

Protection vs. Availability

- Changing Risk Profile
- Porous Perimeters
- Threat Landscape

Information governance = holistic platform for balancing

- Executive Support
- Cross-Functional Team Involvement
- User Awareness and Empowerment
- Policy Enforcement

The People Side of Cybersecurity

- *"Culture eats strategy for breakfast."*
  - Peter Drucker, Management Consultant

➢ Start with what makes sense for YOUR culture
  - After risk assessment!!

➢ Risk-based decisions = strategy

➢ Consider pilots (by role, geography, department)

➢ Consider Attorney-Client Privilege "protection"

➢ Consider baseline metrics for benchmarking, efficacy and continuous improvement

Cybersecurity People Checklist

- Code of Conduct
- Policy/Policy Suite (e.g., Standards, SOPs, WI)
- Communications
- Training
- Employee Engagement (Awareness Building)
- Monitoring, Audits
- Metrics, Effectiveness

➢ Organizational Change Management

Cybersecurity Governance Policy

- Policy statement
- Scope (subject matter; role/level; geography; data type)
- Requirement of good data stewardship
- Other requirements
- Roles and responsibilities
- Accountability
- Consequence management
- External version?

Cybersecurity Communications

- Theme/Red Thread
- Overview of program benefits
- Describe WIIFM (What's In It For Me)
- Explain policy requirements
- Highlight any behavior changes
- Pre-wire future plans
  - Assessment of effectiveness (is that self-assessments, monitoring, audits or employee opinion surveys?)
  - Continuous improvement
  - Additional technology

Cybersecurity Employee Engagement

- In-person instructor-led
- Self-service or instructor-led computer-based
- Gamification
- In-person events (security fairs, socials, demos, give-aways, games, quizzes)
- Remote events
- Role-based/level-based (executive and staff)
- Geography-based
- Languages?
- Frequency?

What is Data Classification?

- Framework
- Foundation for data management
- All data is not created equal - not of equal value
- More Art than Science?
- What is information governance?

"Information governance is the activities and technologies that organizations employ to maximize the value of their information while minimizing associated risks and costs." – Information Governance Initiative Annual Report 2015 - 2016

Why Data Classification? Why Now?

- Data classification standard = implementation of information governance policy
- All data management/protection

  initiatives = implementation of policy

➢ Efficient data management (e.g., IT

  deployments, litigation preparedness)

➢ Increased employee productivity

➢ Increased employee awareness > action

➢ The biggie: Increased data protection

Developing a Data Classification Standard

- *Top Considerations -*
- Purpose(s) of standard
- Will labels/categories be directive, intuitive, aspirational?
- Will categories represent company mission, risk/tolerance and culture?
- What is to be changed? What do you want employees to do?
- Any other objectives at play? For example:

> Replacing another standard > prevent confusion?

> Merging with another company>

> Anticipate new data types or different operations?

Data Classification Standard Challenges

- Label for default?
- Label for trusted advisors?
- Label for benchmarking?
- Label for specific business units/processes?
- Reconciling with former labels
- Auditing and assessment
- Enforcement technologies (e.g., DLP – data loss prevention)

Building Data Classification Awareness

- Tools
- Communications
- Training
- A few thoughts:

➢ Whether data classification is part of company's overall data management/protection strategy

➢ Re-consider role of data classification in company's strategy

➢ Re-consider employee's role in company's data management/protection strategy

➢ Communicate those decisions/considerations
  - ➢ Early and often > consider benchmark metrics
  - ➢ Did you move the needle with comms? Did you build awareness? Change behavior? Increase adoption?

- Real-Life Organizational Change Management Example (Dell)

Typical Business Issues

Transformation from **hardware seller** to **end-to-end IT solutions** and services provider

Your Company Here

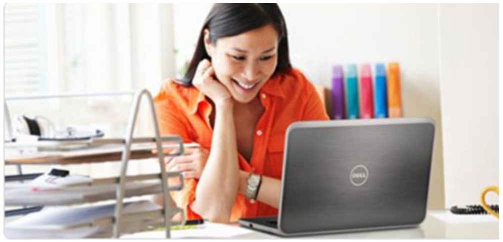
Persistent threat to **confidential information** including **intellectual property**

Further integration of **information management** best practices > **enhancing company’s information management culture**

DELL’s Data Protection Goals

CLASSIFICATION = ONE STEP IN DELL’S DATA PROTECTION STRATEGY

KNOW WHAT DELL HAS SO IT CAN BE MANAGED



DEVELOP DELL’S DATA CLASSIFICATION STANDARD

Data Protection Goals

DEFINE DELL’S DATA CLASSIFICATION LABELS

EDUCATE AND TRAIN TEAM MEMBERS

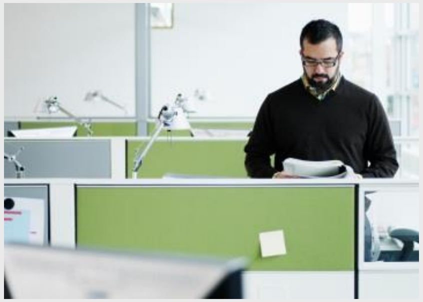
DEPLOY CLASSIFICATION TECHNICAL CONTROLS TO DELL TEAM MEMBERS

Why Data Classification at Dell

Enabled Dell's implementation of its data classification standard

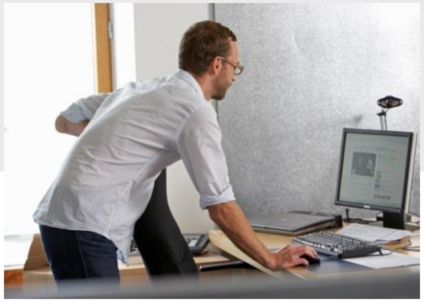
Enabled the classification of information that Dell's employees typically handle

Enabled the continuation of building employee data protection awareness



Empowered employees to classify information for appropriate handling

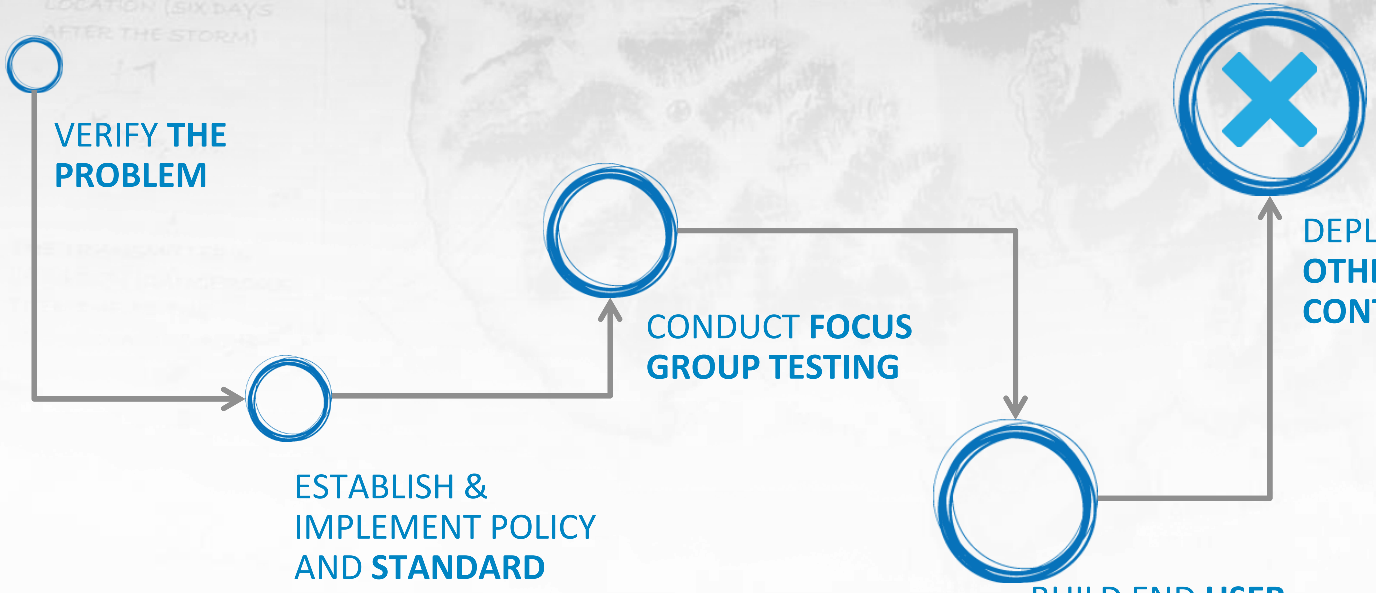
Set the foundation for future data protection initiatives, e.g., DLP (data loss prevention)



Set the foundation for classification enforcement

Component of Dell's Information Governance/Data Protection Journey

DELL’s Data Protection Journey



VERIFY **THE PROBLEM**

ESTABLISH & IMPLEMENT POLICY AND **STANDARD**

CONDUCT **FOCUS GROUP TESTING**

BUILD END **USER AWARENESS** & **INVOLVE USERS** IN DATA PROTECTION

DEPLOY **DLP** AND **OTHER TECHNICAL CONTROLS**

Data Classification Labeling Tool – Sample Comms Plan

January - Get Ready

- Communication to employees to introduce data labeling tool concept
- Communication targeted to executives to ask for participation in tool pilot

February - Be Ready

- Training for executives deployed and recorded for executive pilot
- Communication targeted to executives to encourage them to watch recorded training as needed
- Communication to employees on success of executive pilot

March - Get Trained

- Communication to employees on upcoming tool training dates
- Training deployed to employees
- Communication on tool demos
- Communication on open support dates

April - Start Labeling

- Training ongoing to employees
- Tool demos
- Communication to employees on tool launch dates per region, reminder of recorded training and additional resources on tool support center (microsite)

DELL’s Multi-Layer Communication/Training Plan

KEY

Holistic organizational change management strategy

- Regular communications
- Self-study training videos posted on “TITUS Support Center” webpage
- Global in-person social events to promote deployment (15 sites worldwide)
- Badge card with classification labels and tool information
- Open support sessions 2x weekly (in 2 time zones) to support training
- Use of social media to share user experiences

The Road Ahead…?

- DLP Interlock
- Encryption Interlock
- Endpoints/Mobile/ BYOD

- Regulatory Compliance
- Emerging Technologies

Key Take-Aways

- People are the weakest link in the controls process
- Technology is only a tool; use it to enable holistic information governance
- Data classification is foundation to information governance (not all data is created equal)
- Understand value and power of data classification (data privacy, data protection and data management – retention/disposition)
- Data protection is a journey…

➢ A journey that begins with understanding:

➢ Your company's risk/tolerance and culture

Some “Cybersecurity” Laws

I. Cybersecurity Act of 2015

II. Privacy Law
  - Breach Response Laws (State)
  - Electronic Communications Privacy Act (ECPA)
  - Stored Communications Act (SCA)
  - Computer Fraud and Abuse Act (CFAA)
  - European Union
  - ROW (Rest of World)

III. Employment Law
  - United States
  - European Union
  - ROW (Rest of World)

IV. Litigation (next page)

V. Information Governance (next page)

Some “Cybersecurity” Laws, cont.

IV. Litigation (Litigation Hold/Preservation)

- Federal Rules of Civil Procedure 26(b) and 34:
  “possession, custody or control”

V. Information Governance Examples:

- Records Retention
- Data Disposition
- Data Security
- NIST (National Institute of Standards and Technology) Framework
- PCI (Payment Card Industry)
- Health Data (HIPAA)
- The alphabets (FTC, FCC, SEC, GLB, FFIEC, FDIC, OCC)

- Note: Above are U.S.-centric; ROW applies if xUS data involved
- Note: There are tons of free resources available

Key: Risk-based approach appropriate for your company

THANK YOU!!

Deborah Butler, Esq.
dbutleresquire@gmail.com

Opinions expressed are solely those of the presenter, not Dell's.