Safe Guarding Critical Assets

Outside-In or Inside-Out?

Illini Chapter of ISACA
Sajay Rai, CPA, CISSP, CISM
President and CEO, Securely Yours LLC
sajayrai@securelyyoursllc.com
September 26, 2013

Agenda

- What is a data breach?
- Outside-In Vs. Inside-Out
- A Practical Approach
- Data Classification
- Data Loss Prevention
- Q&A

What is a data breach

According to Wikipedia:

"A data breach is a security incident in which sensitive, protected or confidential data is copied, transmitted, viewed, stolen or used by an individual unauthorized to do so.“

Data breach incidents cost US companies $188 per compromised record, with an average total per-incident cost of $4.8m —
Ponemon Institute study of 2013 (Sponsored by Symantec)

The cost of a data breach – not just $s

- Loss of competitive advantage
- Brand Damage
- Loss of reputation
- Litigation/Legal possibilities
- Fines, penalties, sanctions and regulatory action
- Loss of customers
- Impact on Shareholder value
- Cost of compliance

Top 2013 Data Breaches so far

Source: SC Magazine

Breach	Additional Information
Living Social	Daily-deal website LivingSocial confirmed that its computer systems were hacked, resulting in “unauthorized access.” The company updated its password encryption method after the breach impacted more than 50 million users. Names, email addresses, dates of birth, and salted passwords were stolen.
Washington State Office of the Courts	After the public website of the Washington state Administrative Office of the Courts was hacked, sensitive data of individuals whose cases were making their way through the state court system was compromised. Names, Social Security numbers, and driver’s license numbers were accessed.
Evernote	The popular notetaking software service Evernote had to reset the passwords of all of its 50 million users following a network breach. The company did not find any indication that content or payment information was stolen. Usernames, email addresses, and encrypted passwords of users were accessed.
Drupal.org	The servers of the open source content management platform were hacked, and the sensitive information of close to one million accounts was stolen. As a safety measure, the company reset all passwords. Usernames, email addresses, country information, and hashed passwords were all exposed.
Federal Reserve Internal Site	The Fed admitted that hacking collective Anonymous breached one of its internal websites, accessing the personal data of 4,000 bank executives. Mailing addresses, phone numbers, business emails and fax numbers were accessed and published by the hackers online.

Top 15 Data Breaches

Breach	Date	Additional Information
Heartland Payment System	Mar 2008	134 million cc – SQL Injection
TJX Companies Inc.	Dec 2006	94 million cc – Weak Encryption
Epsilon	Mar 2011	Millions of records - Phishing
RSA Security	Mar 2011	40 million records - Phishing
Stuxnet	2007-10	Intrusion template - nuclear
Dept of Veteran Affairs	May 2006	26.5 million records - Encryption
Sony Playstation Network	Apr 2011	77 million records
ESTsoft	Jul 2011	35 million South Koreans
Gawker Media	Dec 2010	1.3 million records bloggers
Google	Mid 2009	Stolen Intellectual Property
Verisign	2010	Undisclosed information
Card Systems Solutions	2005	40 million cc
AOL	Aug 2006	20 million records – human error
Monster.com	Aug 2007	1.3 million records - Phishing
Fidelity Information Service	Jul 2007	3.2 million records – Access Cont.

Other Topics related to data breaches

- NSA (Snowden)
- Wikileaks
- Syrian Electronic Army hacks US Marines site

Why are data breaches happening?

- Spending more on security since the last decade
- Awareness has increased many fold
- Better detection and monitoring tools
- More resources dedicated to security within an organization
- Vendors are providing integrated security solutions

So, why are these data breaches still happening?

Where is our focus?

- Firewalls
- IDS/IPS
- Traffic monitoring
- Packet sniffing
- Content Filtering

- FOCUS IS ON EXTERNAL THREATS (OUTSIDE-IN)

Outside-In

- External Threat Focus
  - By software developers (Firewalls, IDS, IPS)
  - By organizations (thought that the perpetrator is from outside)
  - Majority of security budget spent on perimeter protection
  - Easier for software vendors to sell the perimeter products as it can be a turn-key solution
  - Organizations like this approach because it gives them a sense of protection with least effort

Outside-In

- Common Myths
  - No breach occurs from within
  - Internal employees have good security awareness
  - Bad guys are all outside the network

Outside-In

- Most organizations now agree that perimeter will eventually be PENETRATED
- The percentage of spend on security MUST SHIFT
- The SHIFT to Inside-Out

Shift to Address these data breach Incidents

- SSNs leaving via email and web traffic
- Credit card numbers sent via email and web traffic
- Employee contract with salary and employment terms sent in clear text and stored on an open share
- SSN and CCN stored on open file share
- Corporate contract terms with major partner circulating in clear text
- Customer SSNs entering and leaving via monthly call center report indicating broken business process
- Credit card numbers sent in email body to personal and corporate domains (hotel confirmations for upcoming conference)
- Promotion and new product material sent in clear text
- Corporate sales proposal and existing plan data sent unencrypted
- Weekly bankruptcy status report sent inbound from business partner
- Selling strategy document leaving unencrypted
- Three-year financial forecast sent in clear text

Inside-Out Concepts

- Focus on “crown jewels”
- Layered concept of protection
- Typically, 5% or less of all data
  - Trade secrets, customer data, pricing data

Inside-Out

- Shift started few years back due to focus on privacy laws
  - HIPAA required protection of PHI
  - GLBA required protection of PII
  - PCI required protection of CC
- Vendors rushed to bring focus on protecting PHI, PII and CC information
- DLP concept was introduced
- Turnkey solution was made available
  - Out of the box, protects PHI, PII and CC

Inside-Out – What Next

Two “old” concepts are becoming in vogue again

- Data Loss Prevention
- Data Classification

Inside-Out – DLP

- DLP is mature software now
- Most organizations still using it for turnkey PHI, PII and CC
- Majority of “crown jewels” still not under DLP
  - “crown jewels” details unknown

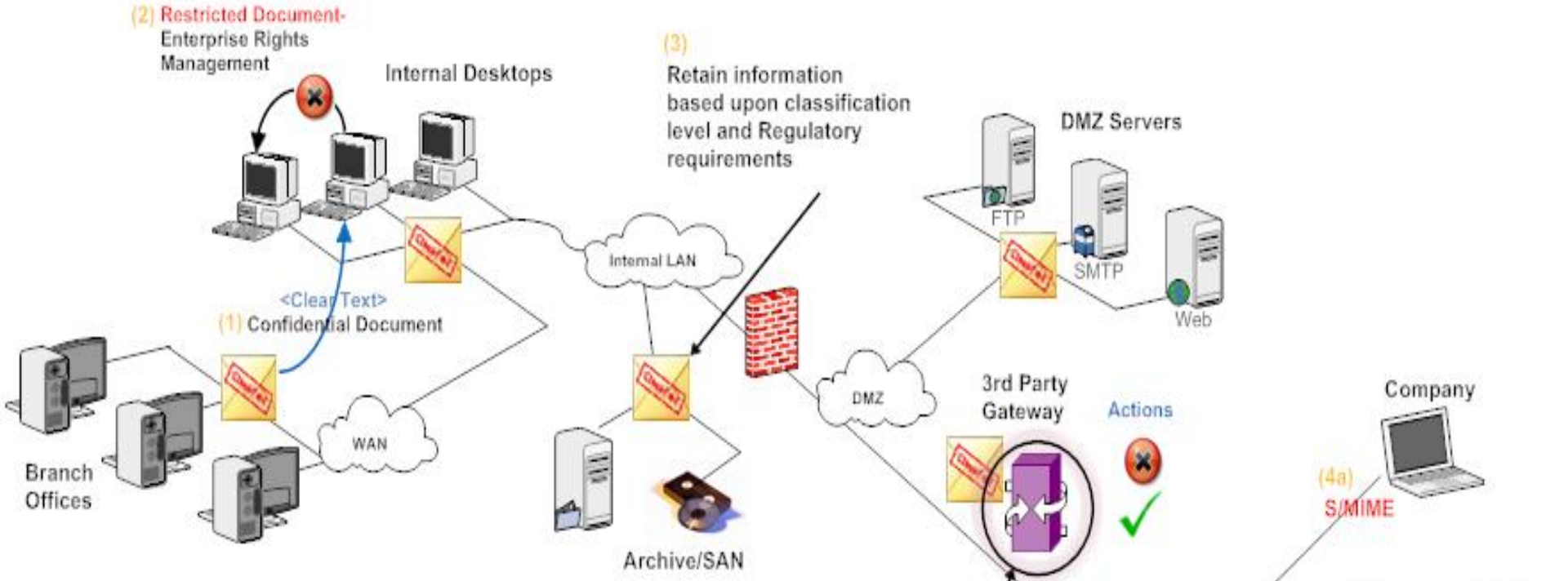
DATA CLASSIFICATION is the critical element

Inside-Out – Data Classification

- Every Organization has Data Classification Policy
- Some Organization has Data Classification procedures
- Majority of Organizations do not classify their data
  - And if they do, they do it at a very high level
  - And even if they do, most employees do not understand the use of it

Data Classification – Use Cases

Classification of Data, based upon sensitivity and criticality, can enable other technology solutions to leverage classified information to ultimately make decisions (transparent to the user) based upon policy



Use Cases:

(1) User sends a confidential document to an authorized user. Based upon the context of the destination, supporting technology allows the e-mail to be sent in clear text.

(2) User sends an un-authorized user a 'restricted' document. Based upon policy, ERM is invoked, and blocks the e-mail/document.

(3) Based upon documents / e-mail which are tagged as 'classified' or 'restricted' storage solutions are invoked to enable intelligent archiving.

(4) Based upon the content of the document / e-mail leaving the company, various solutions can be invoked to protect and sustain the classification level.

- **(4a)** If sent to another company, the classified e-mail can be encrypted using S/MIME
- **(4b)** If sent to a partner, the entire data can be encrypted to preserve confidentiality & Integrity.
- **(4c)** If sent to a customer, the customer can be sent a message for pickup, and the pickup can be communicated via a SSL connection.

Where do we start?

- First 3 months of Inside-Out
  - Review/Update the data classification policy (buy-in from corporate executive is critical)
  - Develop a data classification procedure which provides data owners guidance on how to classify data
  - Update the awareness program and roll out to educate owners on how to classify data
  - Identify a DLP solution, which can be customized for organization's classification needs (Most DLP software do a good job of catching PHI, PII and credit card data). DLP software should interface with your libraries.

Where do we start?

- 3-9 months of Inside-Out
  - Deploy the initial DLP software to enable detection of PHI, PII and credit card data
  - Work with two major business units to start identifying corporate “crown jewels” and tag the data (R&D, Legal, Engineering)
  - Ensure the awareness program is completed by data owners
  - Inventory the “crown jewels” and start to understand which software/systems they reside
  - Classify the “crown jewels” and enable DLP

Where do we start?

- 9-12 months of Inside-Out
  - Your organization should have a “working” solution for protecting sensitive data leaving the organization
  - Start to roll out the solution to other divisions
  - Start to incorporate other requirements like export control and other regulatory requirements into the classification process

End goal is to protect classified data

Classify – Determine the appropriate level of classification

Label – Tag the asset with the appropriate level of classification

Protect – Define appropriate security controls commensurate with the classification to protect the asset

Data Classification

- Most of us have good classification policy statement
- Typically, the classification is:
  - Public
  - Internal Use
  - Confidential
  - Secret
- Most users of organizations understand the classification policy but do not know how to use or implement it

Additional guidance / rules (sample)

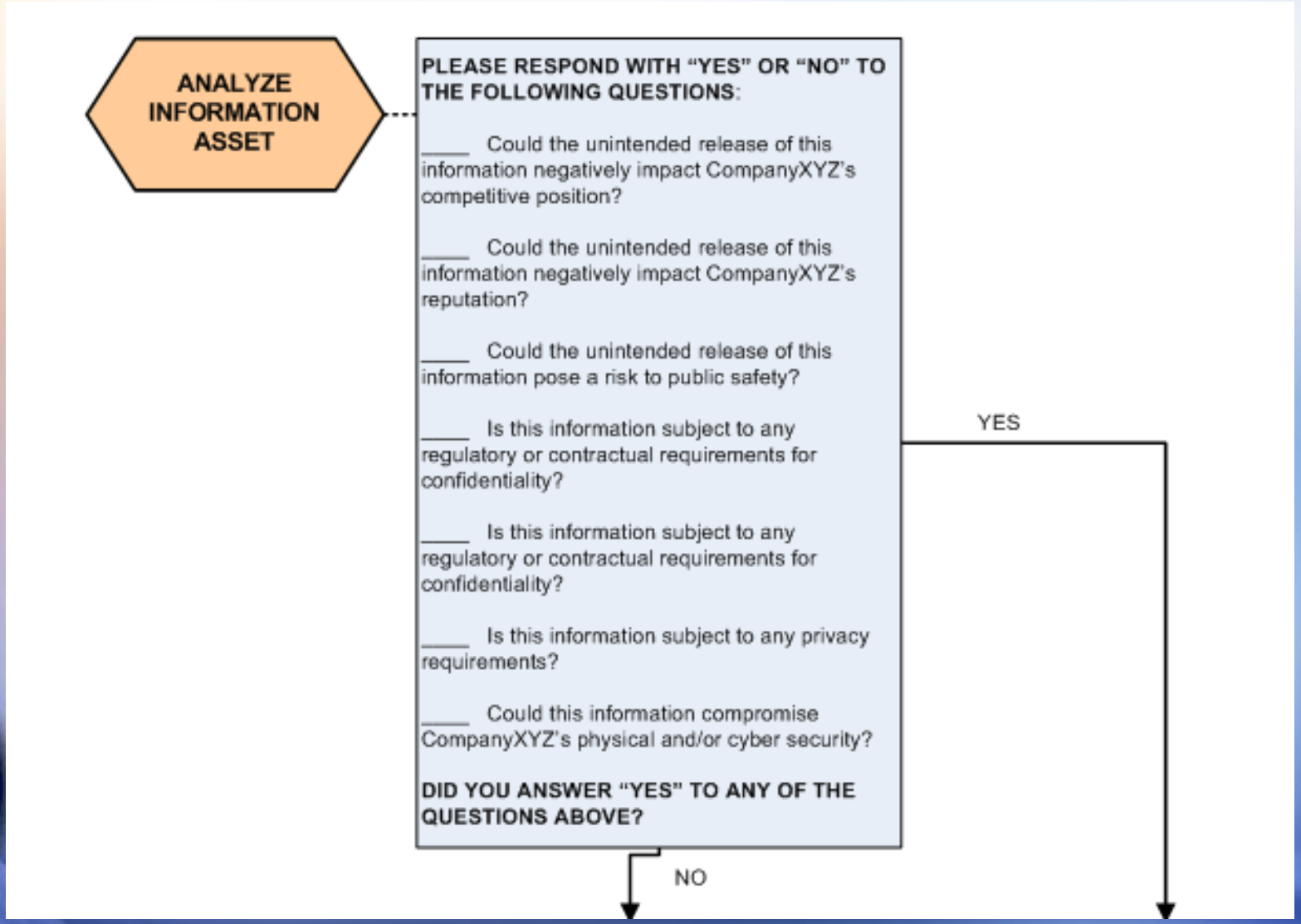
Public	Internal Use	Confidential	Secret
Intended to be shared with the general public, media, or customers	Generally available to all personnel	Available to individuals within your organization who have a business need for access (may be defined by groups)	Available to specific individuals who have a business need for access
Requires approval of Corporate Communications prior to release to the general public	Should not be shared with customers, media, or the general public	Should never be shared with customers, media, or the general public	Should never be shared with customers, media, or the general public
Appropriate to share with government agencies, regulatory bodies, and business partners	May be shared with government agencies, regulatory bodies, and business partners if a business need exists	May be shared with government agencies, regulatory bodies, and business partners if a business need exists and appropriate protective measures are in place	May be shared with government agencies, regulatory bodies, and business partners if a business need exists, protection measures are in place
Appropriate to share with personnel, contractors, and consultants	Appropriate to share with personnel, contractors, and consultants	Appropriate to share with company personnel, contractors, and consultants only if appropriate protection measures are in place	May share with company personnel, contractors and consultants only if appropriate protection measures are in place
May be available on the corporate intranet	May be available on the corporate intranet	Should never be available on the corporate intranet without access control measures	Should never be available on the corporate intranet
May be available on external web sites	Should not be available on external web site without access control measures	Should never be available on company's external web site	Should never be available on company's external web site

Develop examples of Classification

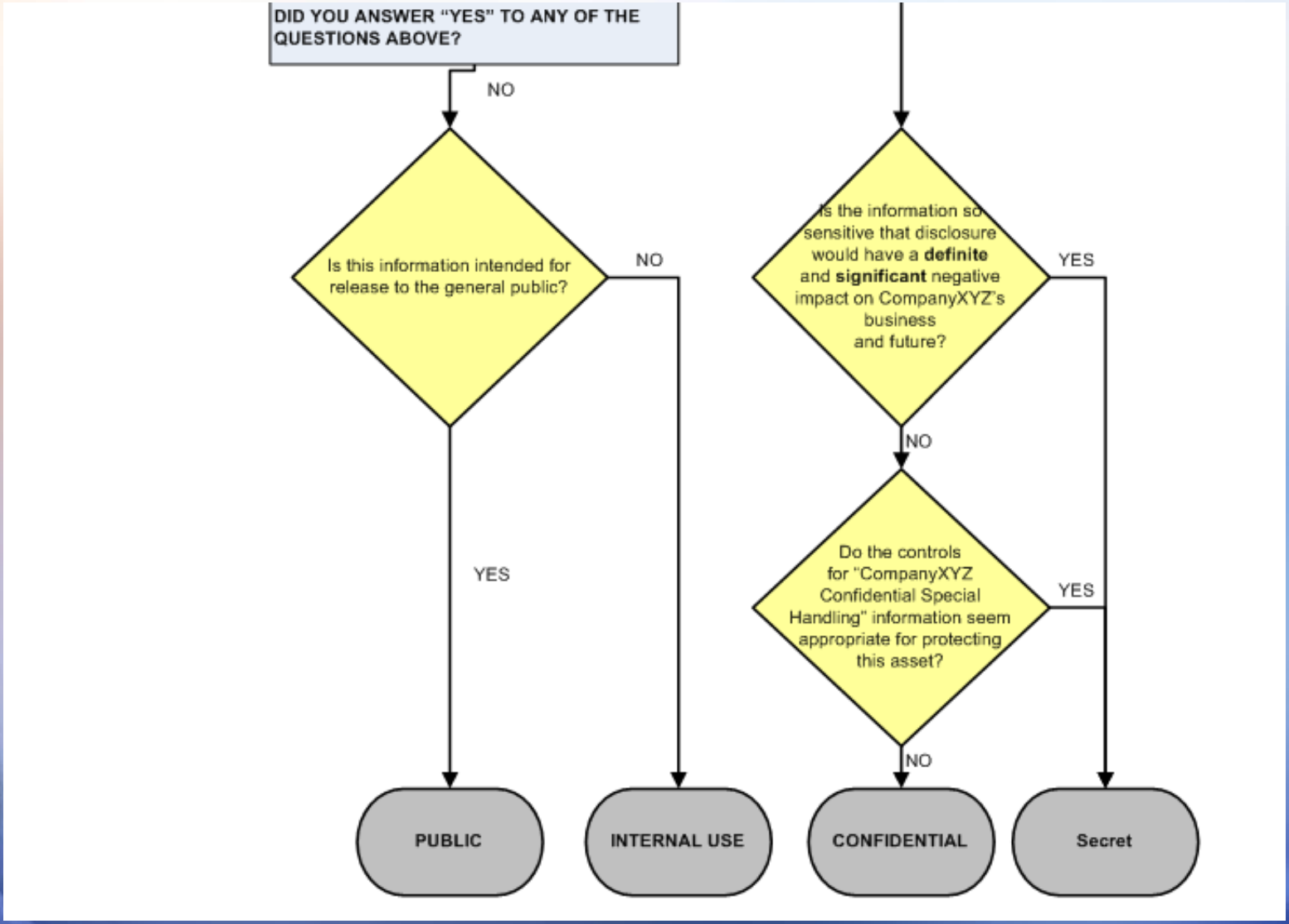
Public	Internal Use
▪ Marketing Materials ▪ Annual Report (after release) ▪ Press Releases ▪ Public Announcements	▪ Policies & Standards ▪ Organization Charts ▪ Facility Maps ▪ Telephone and E-mail Directories

Confidential	Secret
▪ Budgets ▪ Financial Forecasts ▪ Market Studies ▪ Risk Analyses ▪ Network Diagrams	▪ Bid and Proposal Information ▪ Personally Identifiable Information ▪ Attorney-Client Privileged Information ▪ Unannounced Merger or Acquisition Information

Classification process



Classification process



Classification examples

APPENDIX A: RECOMMENDED CLASSIFICATIONS FOR INFORMATION ASSETS

The following examples of common information assets are already classified to simplify the process for you. These recommended classifications are a **minimum** classification.

IMPORTANT: Please classify your information as more sensitive if you feel that is warranted by the content.

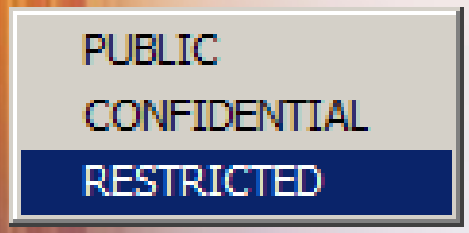
Information Asset Type	Classification
A	
Administrative accounts and passwords	Secret
Annual report (after release)	Public
Annual report (before release)	Secret
Attorney-client privileged information	Secret
B	
Bid and proposal information	Secret
Budgets	Confidential
Building layouts	Internal Use
Business continuity plans	Confidential
C	
Company employee communications sent via email or internal posting	Internal Use
Compliance data of any kind that must by law or regulation be filed with public entities but not yet released by Ciena (e.g., SOX, HIPPA, EPA, NERC, etc.)	Secret
Contract terms	Secret
Corporate business strategies	Confidential

Classification examples

L	
M	
Market studies	Confidential
Marketing materials	Public
Medical records	Secret
Merger & acquisition information (unannounced)	Secret
N	
Network diagrams	Confidential
O	
Operational procedures	Confidential
Organizational charts	Internal Use
P	
Password Repositories	Secret
Payroll data	Secret
Plant maintenance records or logs	Confidential
Policies	Internal Use
Press releases	Public
Project documentation (e.g., requirements, implementation plans, schedules, test plans); depending on the sensitivity	Internal Use
Public announcements	Public
Public utility commission filings	Internal Use
Q	

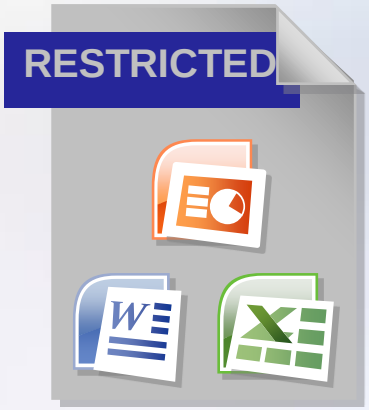
How It All Fits Together

Classify



- **End user classifies file**

Add Metadata



- **Classification should add metadata to the Office document**

Protect

- **DLP solutions enforce policy based on metadata**

Engage the End-User

- Machines cannot classify nearly as accurately as end-users
- Users must understand classifications and data handling. Otherwise data protection efforts tied to classification have limited value
- Direct end-user feedback engages them at the point in which they are executing business processes, which is highly effective
- Some organizations have security or compliance “champions” as outreach to the rest of the organization who can help

Leverage Technology – To Educate

- Educate with tool tips & visual markings
- Label documents with point-and-click ease
- Provide targeted feedback/training directly where and when it's needed, at risky users
- Can avoid costly mistakes – most exposures are the result of mistakes, not malicious acts
- Stop internal documents from being sent outside the organization
- Users get immediate feedback to self-remediate policy violations

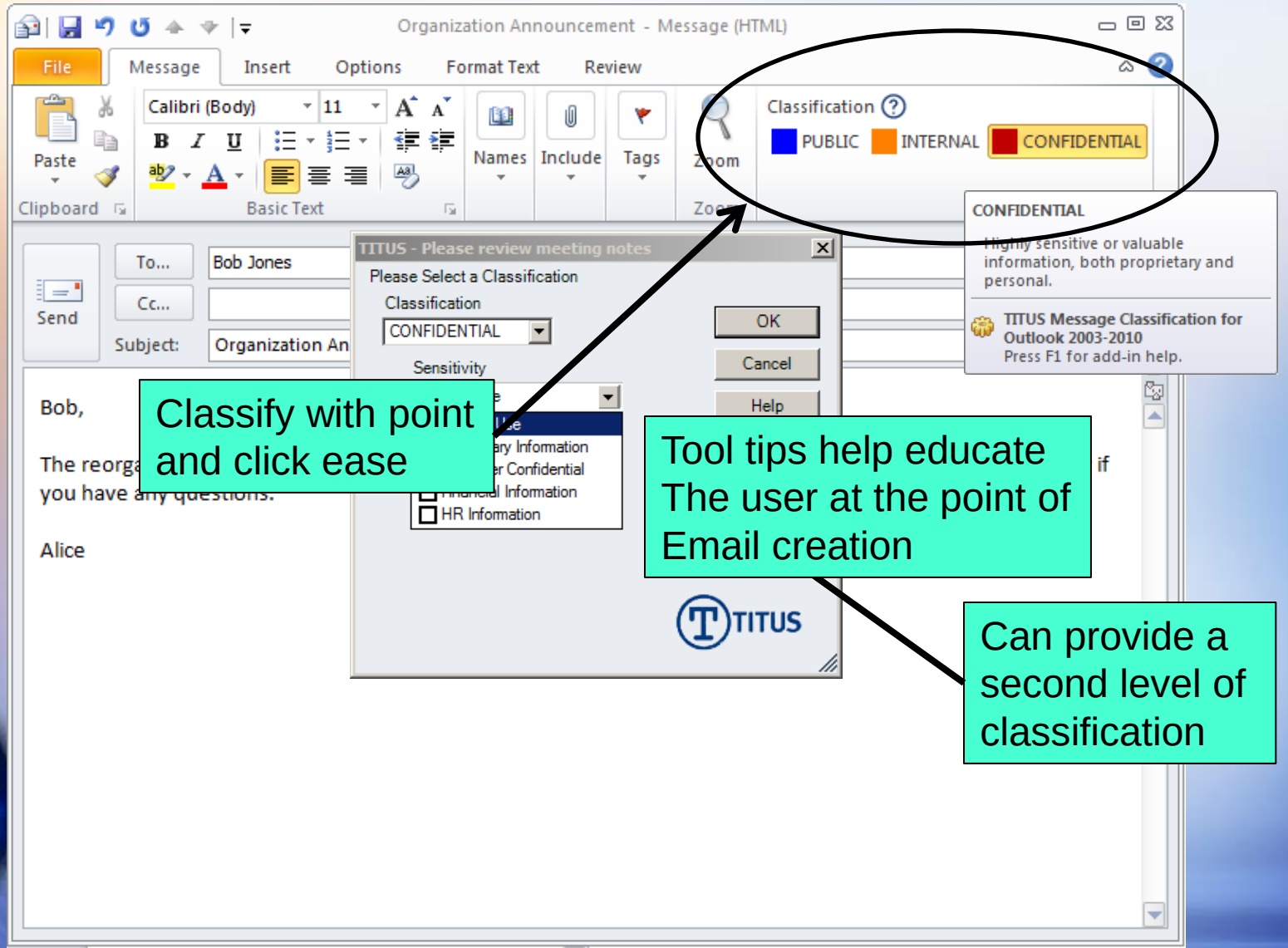
Leverage Technology – To Classify & Label

- Classifying in Outlook means manually adding a header or footer to the email
- Classifying documents in MS Office means modifying the document metadata (properties), which is not simple or intuitive
- Classifying in SharePoint is easier in lists, but not intuitive with document libraries
- Technology can provide ease of classification with point-and-click ease
- Adds metadata tags to better enable DLP capability

Classification in MS Outlook & OWA

- Provides an integrated interface with the Outlook client and Outlook Web Access
- Allows point and click classification
- Tool Tip feedback helps educate users on the classification levels before selecting
- Can apply visual markings in the subject line and/or email body to indicate classification
- DLP/Email Encryption tools can trigger off classification labels, for example “encrypt any outbound email tagged “PHI” or “Secret”

Classification in MS Outlook

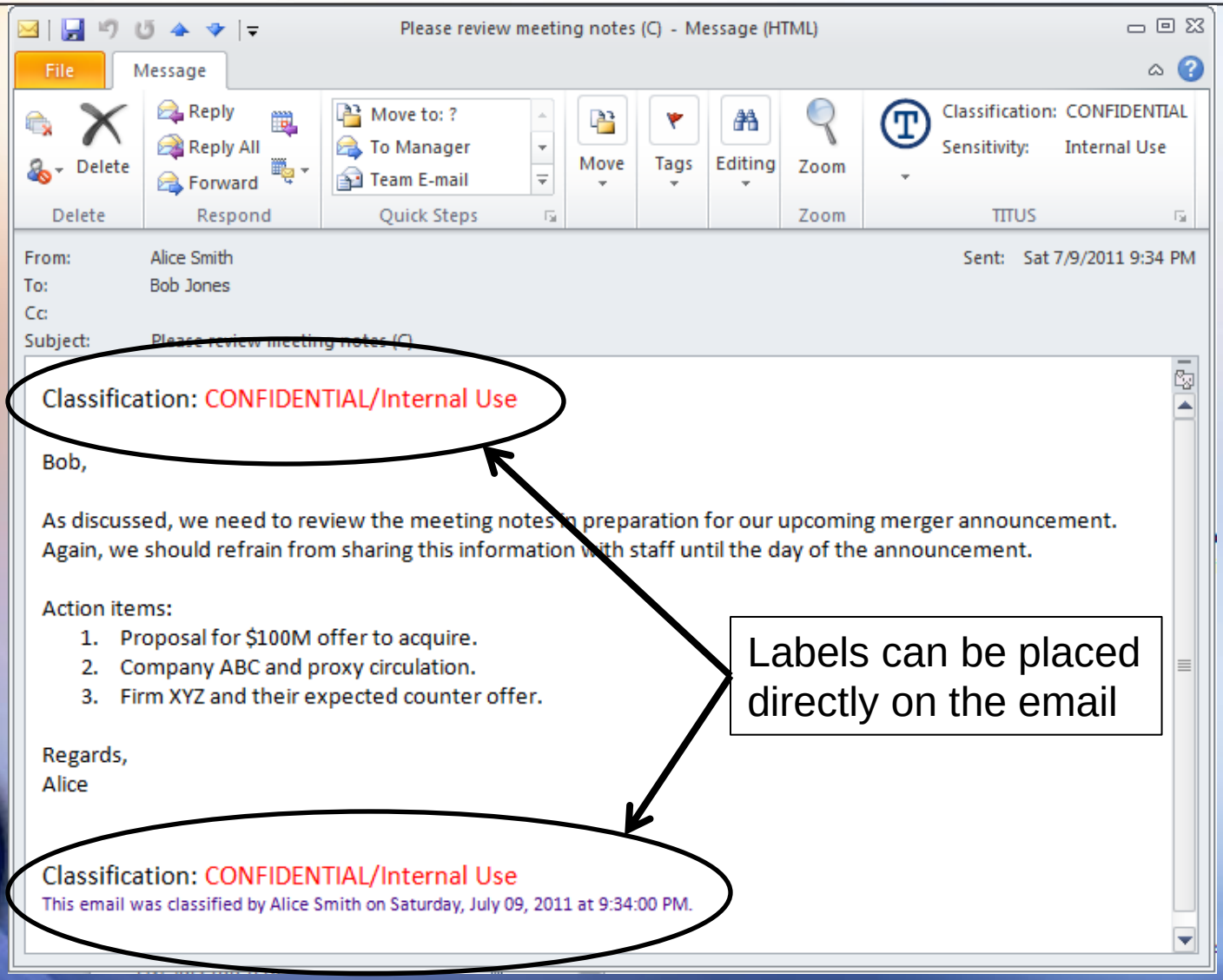


Additional Capabilities

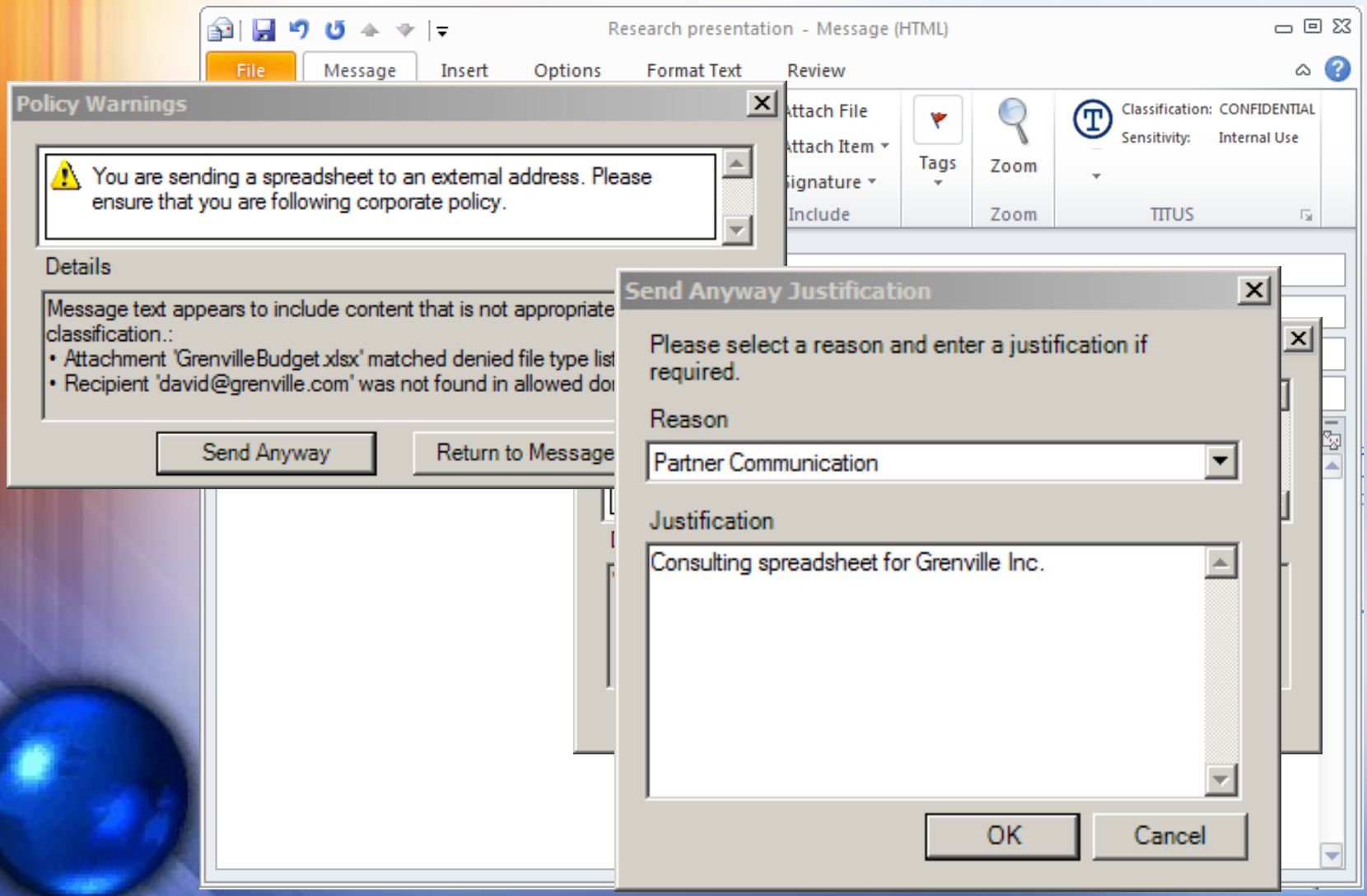
Titus Labs software can provide DLP-like capability within their classification software

- Can verify internal vs. external recipients
- Can prompt when an action does not match the classification
- Can prevent lowering the classification when forwarding
- Can be set to limit the maximum number of recipients
- All messages are customizable

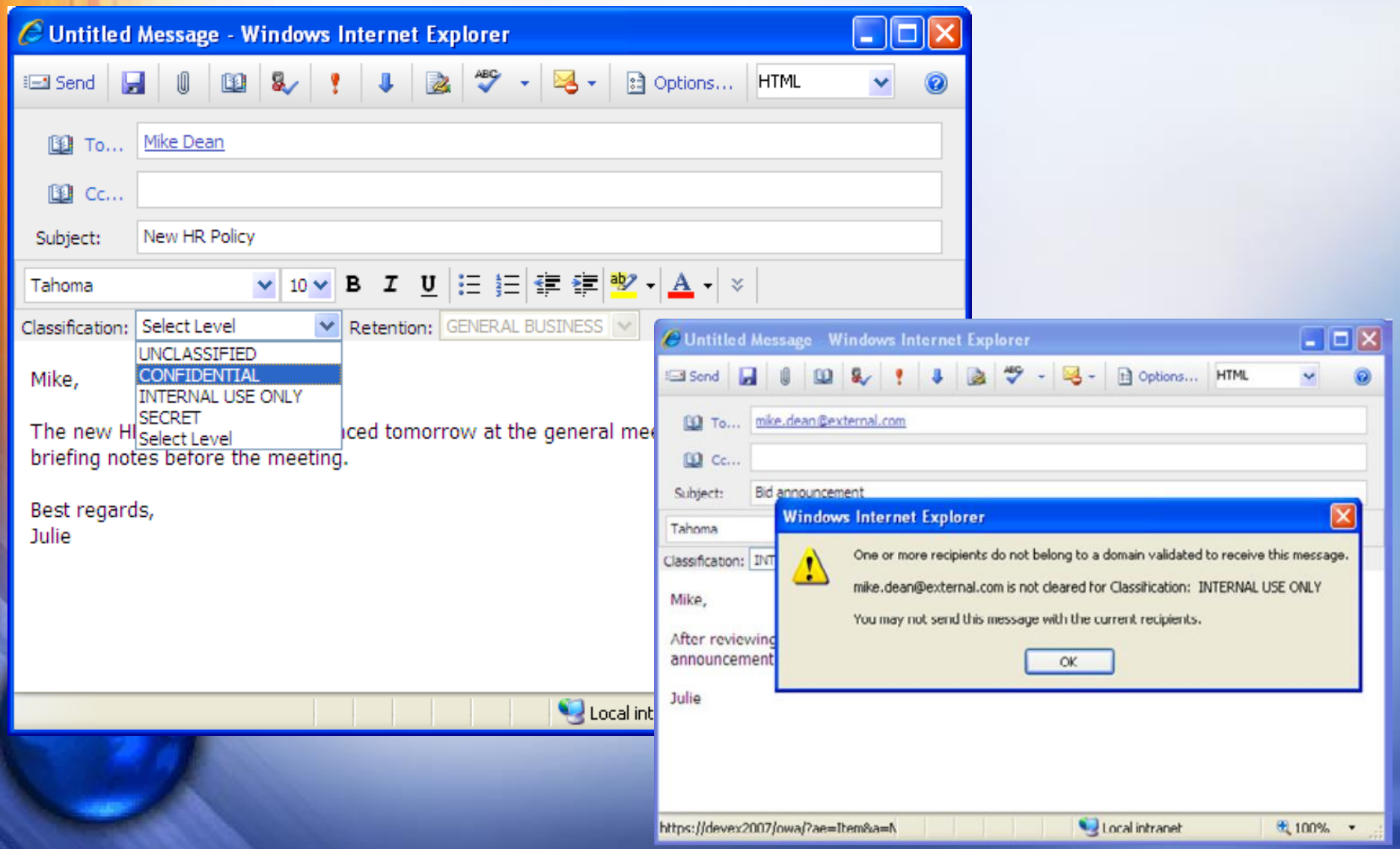
Document Marking



Recipient and Classification Validation



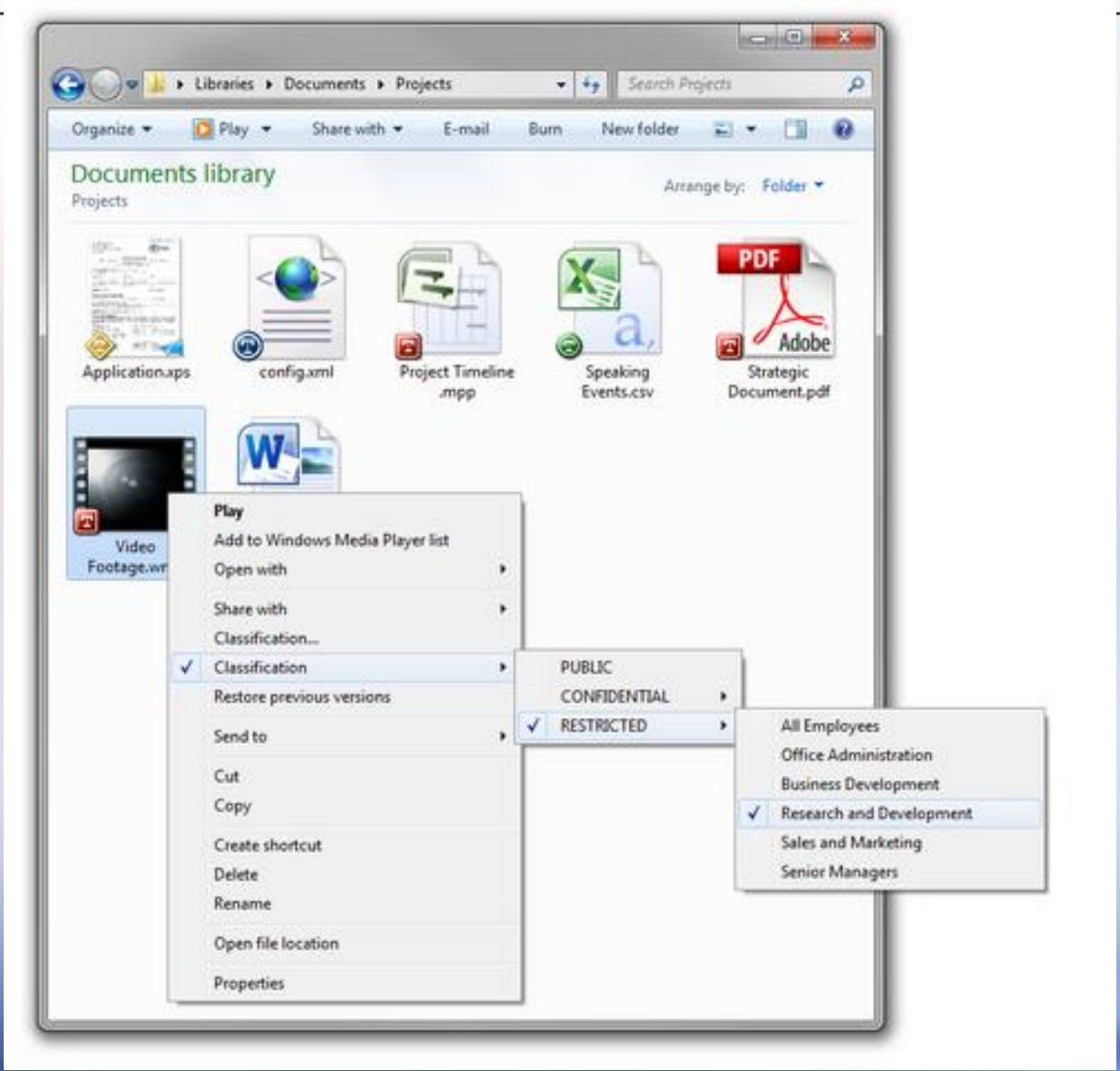
Classification in Outlook Web Access

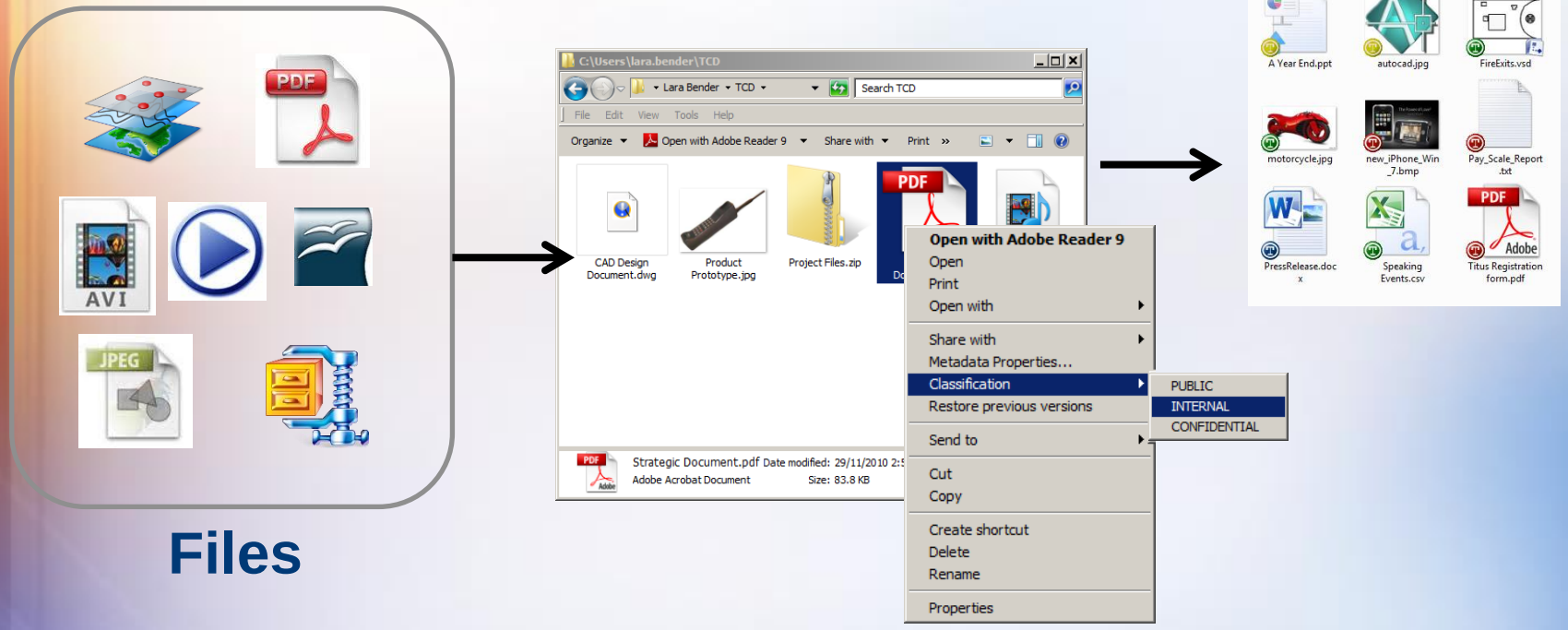


Classification in Windows Desktop

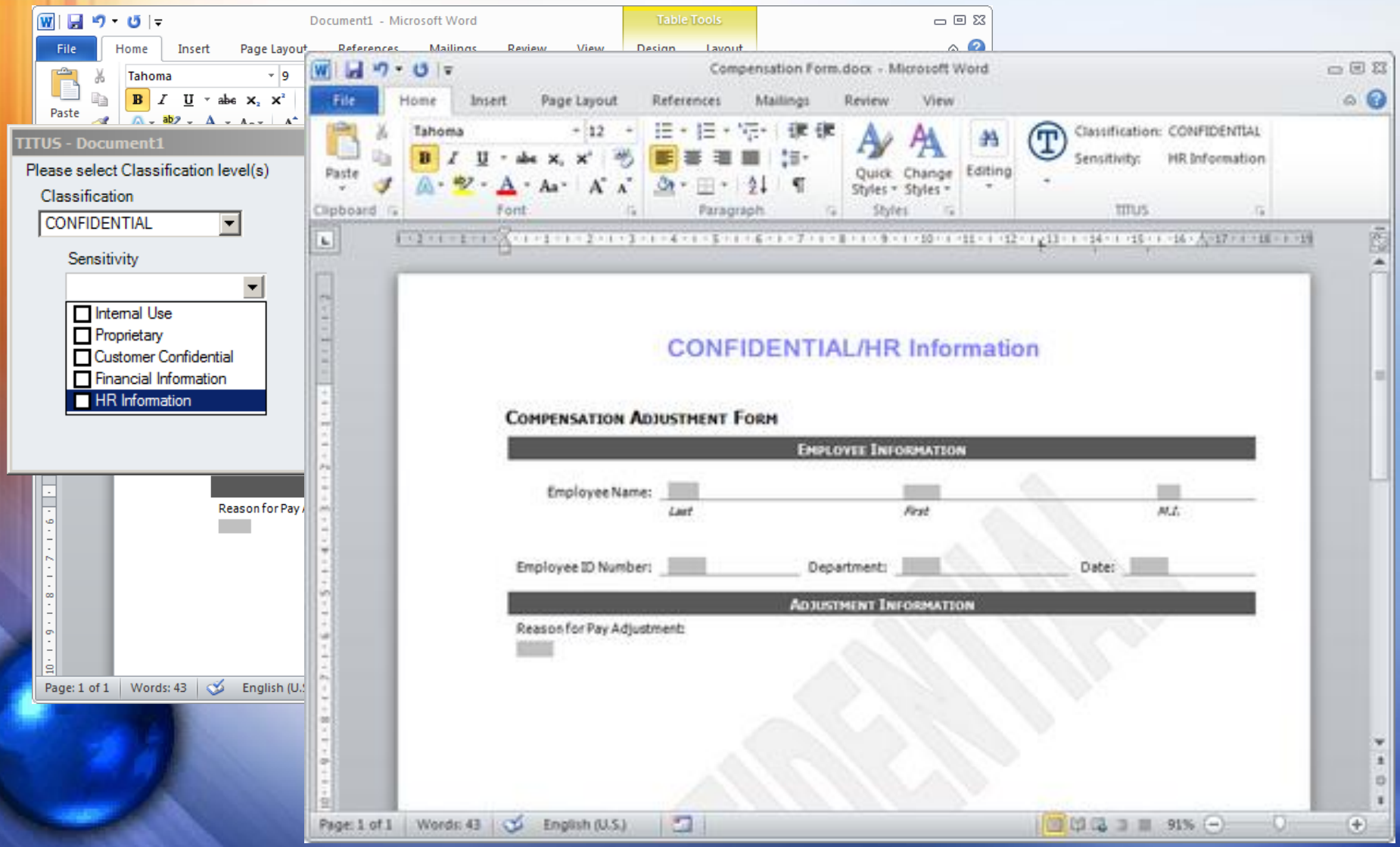
- Integrated UI with Windows
- Can require classification to save a document or email a document
- Color-coded icons visually identify the classification to users
- Can implement 2-stage classification
  - Classification
  - Sensitivity or Retention Period
- Automatically adds to document properties, header or footer per organization intent

Classification in Windows Desktop




PDF
AVI
JPEG
Files
C:\Users\lara.bender\TCD
Lara Bender ▸ TCD ▸
Search TCD
File Edit View Tools Help
Organize
Open with Adobe Reader 9
Share with
Print
CAD Design Document.dwg
Product Prototype.jpg
Project Files.zip
PDF
Strategic Document.pdf Date modified: 29/11/2010 2:5
Adobe Acrobat Document
Size: 83.8 KB
Open with Adobe Reader 9
Open
Print
Open with
Share with
Metadata Properties...
Classification
Restore previous versions
Send to
Cut
Copy
Create shortcut
Delete
Rename
Properties
PUBLIC
INTERNAL
CONFIDENTIAL
A Year End.ppt
autocad.jpg
FireExits.vsd
motorcycle.jpg
new_iPhone_Win_7.bmp
Pay_Scale_Report.txt
PressRelease.docx
Speaking Events.csv
Titus Registration form.pdf

Classification in MS Office

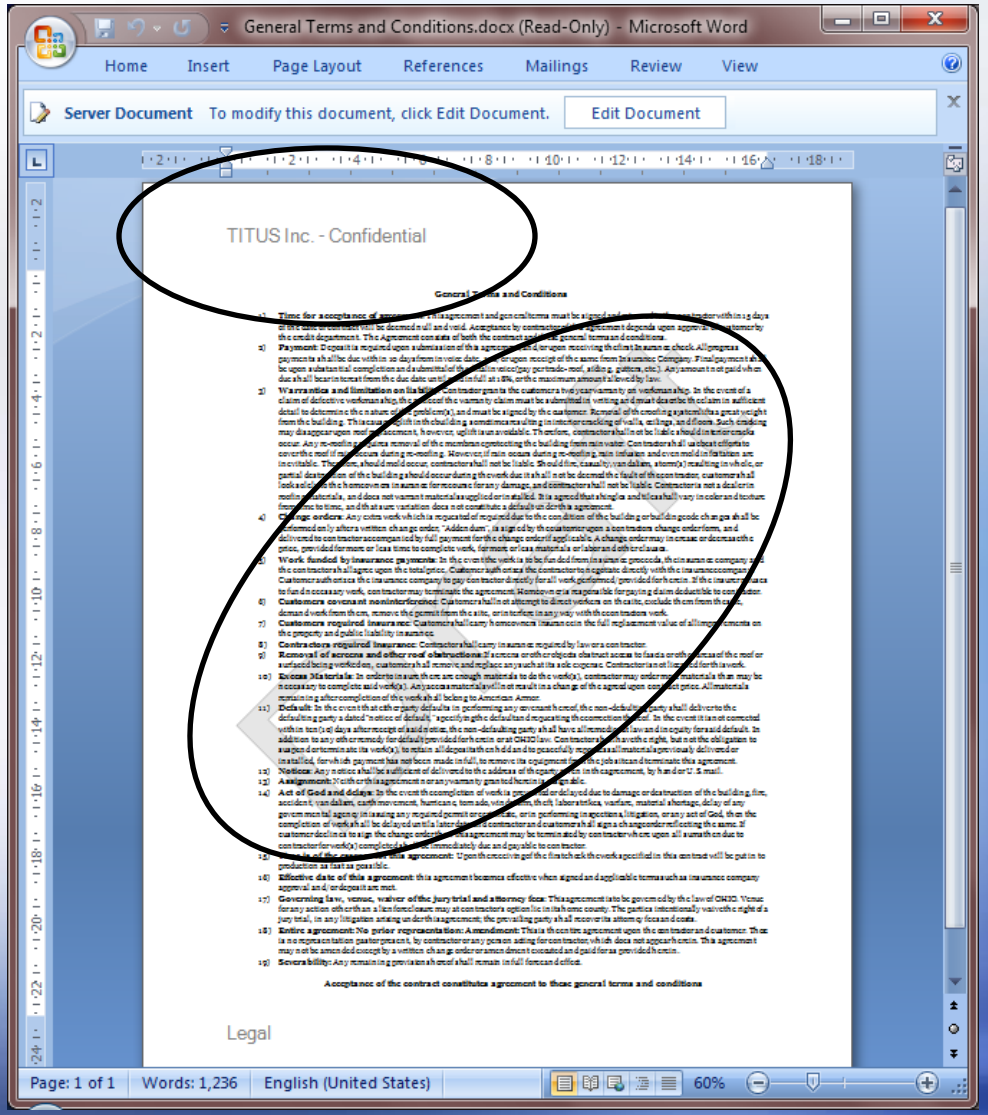


Classification in Sharepoint

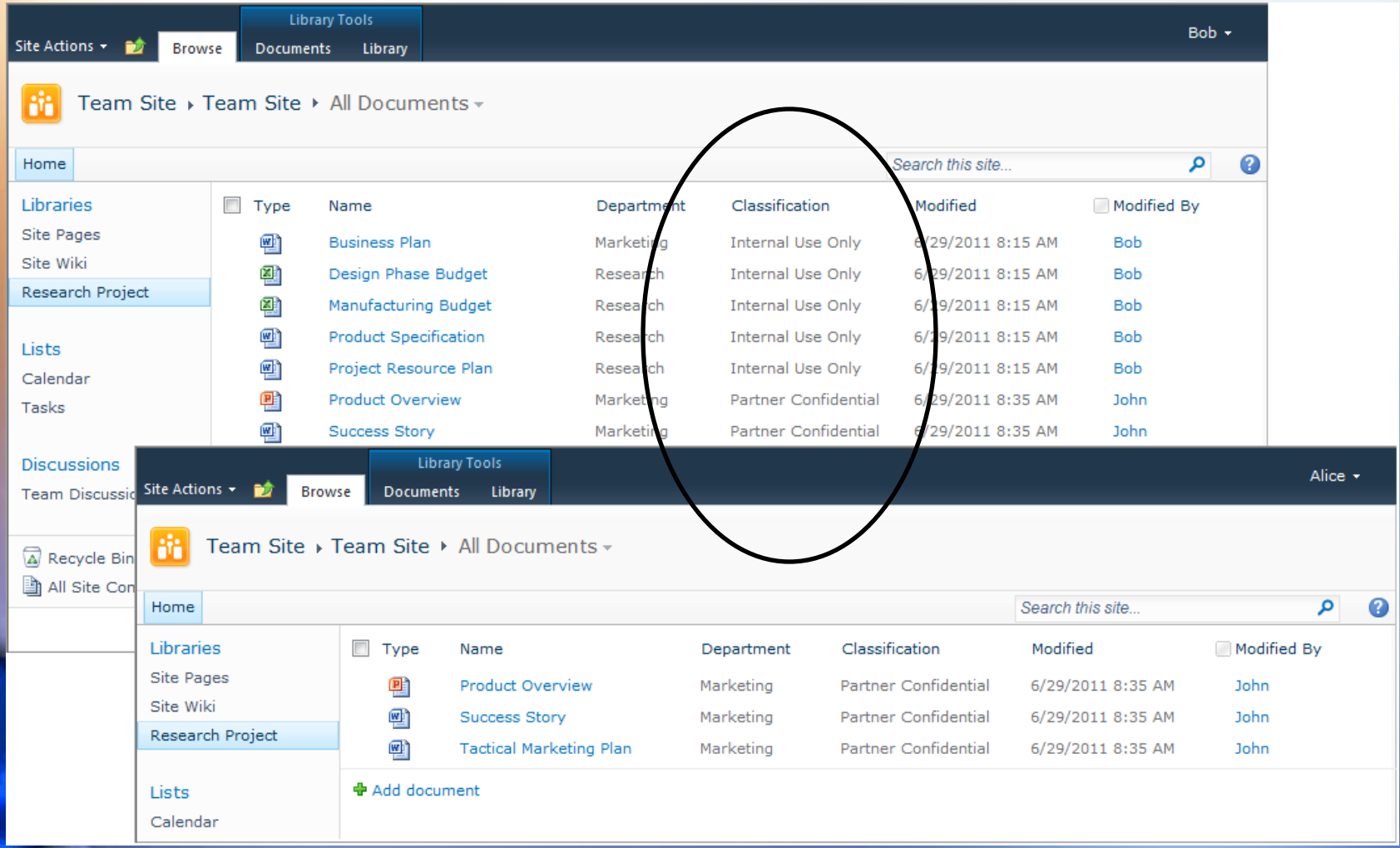
- Provides ability to apply classifications to individual documents in a repository or list
- Can force classification on save or upload
- Allows you to control security on documents according to metadata tags (attributes)
  - For example, Group A can access “internal use only” document, while Group B can access “internal use only” and “confidential”

Classification in Sharepoint

When adding classification to an uploaded document, headers, footers and watermarks can be automatically added

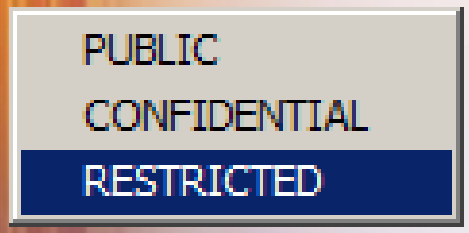


Classification in Sharepoint



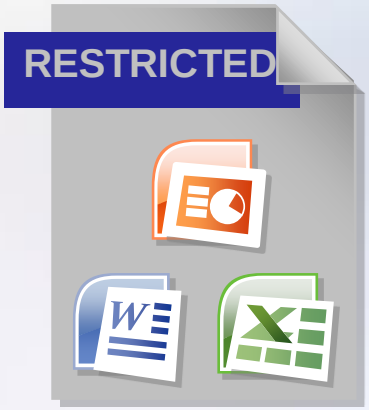
How It All Fits Together

Classify



- **End user classifies file**

Add Metadata



- **Classification should add metadata to the Office document**

Protect

- **DLP solutions enforce policy based on metadata**

What is Data Loss Prevention?

- A layered security control
- A detective control
- An information theft deterrent
- A preventative control if strict rules are enforced (can prevent the action, but not the attempt)
- A data inventory/discovery tool?

Bottom line: A content filtering tool

What Can DLP Identify?

Email

- Sensitive data sent outside the company

Web

- Files attached to webmail (Gmail, Hotmail, etc.)
- Files uploaded to web sites (Dropbox, etc.)

Endpoint

- Data copied to external media
- Data printed

Network Storage

- Data stored on file shares
- Data stored on SharePoint

Defining Key Business Scenarios

It's all about the data…

- Where is it? How is it being used?
- How can I prevent loss of it?
- What scenarios are most important?

Customer, Employee, Patient, Student Data

Regulatory Compliance

- Social Security Numbers
- Credit Card Numbers
- Contact Information
- Health Information

Intellectual Property

Competitive

- Source Code
- Engineering Specs
- Strategy Documents
- Pricing

Company Confidential

Reputation

- Quarterly Results
- M&A Strategy
- CEO Internal Email
- Internal Conversations

Defining Key Business Scenarios (cont.)

Malicious Intent, Mistake or Ignorance?

- Credit cards going to 3rd party via email
- Nurse copying Patient PHI to a USB drive
- Company docs uploaded to SkyDrive
- Bank account numbers stored on an unrestricted file share
- Sending sensitive PII to personal email
- Customer financial information being printed

Once scenarios are defined, business rules can be created to match the requirement

Defining Key Business Scenarios (cont.)

Questions to Ask

- Do regulations dictate unacceptable data transmission (type or method)?
- Do different rules need to apply to different departments? (i.e. it's ok for loan officers to send this data, but not ok for anyone else)
- What situations would trigger a breach response?
- Which scenarios do I only want to view activity for a while to understand "normal" flow vs. which would I react to immediately?

Detecting Classified Data

We've established our classification scheme and implemented a process to classify documents, now how do I prevent data loss?

How Do DLP Rules Work?

- Match described content (pattern match)
- Match exact data (your customer or patients specific data (does not work on endpoint)
- Can match data only, or can require another data element in close proximity (SSN/name)
- Should I care about low or log-only events?
  - YES!
  - Consider which is worse:
    - 1 event of 500 matches (mistake?)
    - or 500 events of 1 match (broken process)

Detecting Classified Data

For classified data:

- Pattern match
  - Find “ABC Secret”
  - Find “Classification: Internal Use Only”
  - Find metadata field Classification with a value of “Secret”
  - *Find outgoing email with property “Internal Use Only”*

Detecting Classified Data

For classified data:

- Proximity match
  - ✓ Find "Secret" within 10 characters of "Classification"
  - ✓ Find *name* within 15 characters of a *credit card number*
  - ✓ Find *name* within 15 characters of diagnosis

Implementation Considerations

Implementation – Business Participation

- Business sponsorship & participation is CRITICAL
- Privacy/Security/Legal/Compliance can determine what situation would constitute a breach per regulations
- What situations would be considered a breach, or indicate a broken process from the business perspective?
- Business should drive thresholds for detection
- Business should be involved in remediation (context)

Implementation – Team Cooperation

- Security Team may flag & filter events
- Privacy will engage in PII incidents
- Security will engage in fraud & IP events
- HR addresses employee actions
- Supplier Mgmt addresses supplier actions
- Cross-company committee provides oversight and approves logical business rules
- Business SMEs approve specific rule criteria

Implementation – DLP Procedures

- Event handling must be defined AHEAD OF TIME
- Who will filter out false positives?
- Who will follow-up on valid events?
- Have SLAs been established based on severity?
    - High
    - Medium
    - Low
    - Audit-only
- Who will make the contact during a follow-up?
- Who will be contacted during follow-up?
  - Manager, Individual

Implementation – DLP Procedures (cont.)

- Do individuals following-up know how to use the DLP tool and manage events?
- Are the security, privacy, fraud incident procedures defined well enough so it's clear when to engage those processes?
- Has HR created procedures to define actions against employees for DLP events?
- What action will be taken against the person?
  - Accidental
  - Negligence (policy violation)
  - Malicious

Implementation – Event Follow-Up

- Now that DLP triggered an event, what should the technology be configured to do?
  - All events are logged
  - Audit – passive, invisible to user
  - Alert – inform DLP team of high priority
  - Notify – popup window to the user
  - Block – popup to user and block the action
- Based upon the number of events, do the responsible teams have sufficient bandwidth to handle the volume?

Implementation – Follow-up Matrix

Sample Decision Table

Network Channel	High	Medium	Low
Web	Block/Alert	Block/Notify	Audit
Secure Web	Block/Alert	Block/Notify	Audit
Email	Block/Alert	Quarantine	Encrypt
FTP	Block/Alert	Block/Notify	Audit
Printer	Block/Alert	Block/Audit	Audit
Mobile (ActiveSync)	Block/Notify	Block	Audit
Custom	Block	Block/Notify	Audit

High/Med/Low thresholds are defined unique to the business

Implementation – False Positives

- They WILL happen (and a lot of them!)
- Exact data matching has fewer

- Common Causes:
  - Numbers resemble SSN or MRN
  - Rule is too broad or has no proximity terms defined
  - Printing trigger data is an approved business process
  - Email was encrypted, but DLP sees it first

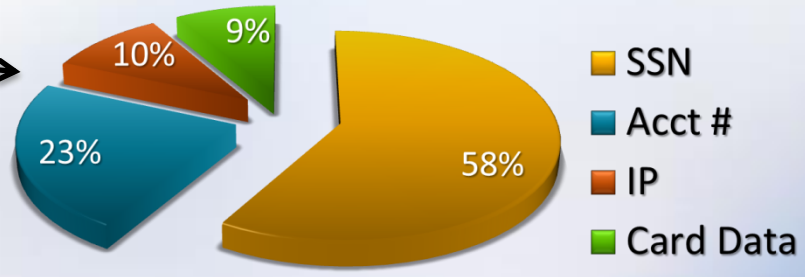
Implementation – Broken Processes

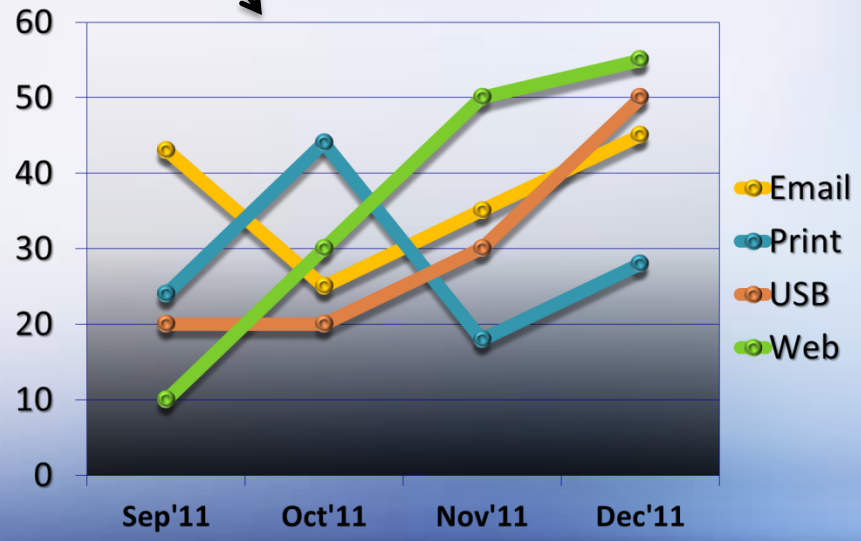
- People don’t realize they’re doing it
- Claim policy ignorance (didn’t know I couldn’t)
- People email or copy docs to work on at home
- Access controls aren’t working as intended
- People steal customer data when they leave
- Repetitive events often indicate broken business processes or lack of adherence to policy

Tracking Risks to Critical Assets

Monitoring Metrics

- Events by Rule
- Events by Loss Path
- Trends by Severity





Tracking Risks to Critical Assets

Monitoring Metrics

- Largest offenders by individual or dept.
- Events by specific asset:
  - Specific files
  - Specific locations
  - Specific classifications