Lotusphere2012

Business. Made Social.

BP204 Smart Plays with Compliance

Bill Malchisky Jr. |
Managing Partner/Chief Technical Architect |
Effective Software Solutions, LLC

Legal disclaimer

The information contained in this publication is provided for informational purposes only. While efforts were made to verify the completeness and accuracy of the information contained in this publication, it is provided AS IS without warranty of any kind, express or implied. In addition, this information is based on IBM's current product plans and strategy, which are subject to change by IBM without notice. IBM shall not be responsible for any damages arising out of the use of, or otherwise related to, this publication or any other materials. Nothing contained in this publication is intended to, nor shall have the effect of, creating any warranties or representations from IBM or its suppliers or licensors, or altering the terms and conditions of the applicable license agreement governing the use of IBM software.

References in this presentation to IBM products, programs, or services do not imply that they will be available in all countries in which IBM operates. Product release dates and/or capabilities referenced in this presentation may change at any time at IBM's sole discretion based on market opportunities or other factors, and are not intended to be a commitment to future product or feature availability in any way. Nothing contained in these materials is intended to, nor shall have the effect of, stating or implying that any activities undertaken by you will result in any specific sales, revenue growth or other results.

Performance is based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput or performance that any user will experience will vary depending upon many factors, including considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve results similar to those stated here.

IBM, the IBM logo, Lotus, Lotus Notes, Notes, Lotus Mobile Connect, and Lotusphere are trademarks of International Business Machines Corporation in the United States, other countries, or both. Unyte is a trademark of WebDialogs, Inc., in the United States, other countries, or both.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both. Other company, product, or service names may be trademarks or service marks of others.

THE VIEW is a trademark of Wellesley Information Services All rights reserved.

Information Technology *Adviser* is a trademark of Progressive Business Publications

Good Technology is a trademark of Good Technology, Inc.

All references to "Foo", "Foo, Inc.", "Equipment vendor", and "Company" refer to fictitious companies, respectively, and are used for illustration purposes only.

All references to "Jane Doe", "John Doe", "Attorney", "User" refer to fictitious individuals, and are used for illustration purposes only.

Agenda

- Introduction
- Important Compliance Facets
- Culture and Compliance
- Group Discussion – Implementation
- Compliance Case Corner
- Wrap-up

Acknowledgement

- Some of the data in this session is based upon my article in THE VIEW Journal, entitled, “Compliance and the Domino Administrator: Essential Knowledge, Planning, and Journaling”

- For a more detailed review of the subject matter, please see the article located here

  - http://www.eview.com/eview/volr6.nsf/0/C127726767FA2A77852578860055 39F9?opendocument

  - Note: subscription required

Disclaimer

All information in this session is provided as is. You are free to use it within your organization, and plan internally with no express written or other implied warranties. No one connected with Lotusphere® is responsible for your environment. If there are any questions on the points presented herein, seek the advice of your corporate legal department. Use at your own risk and you accept all responsibility for doing so.

Additionally, the information in this deck is provided as general information and should not be viewed as legal advice.

Quick Background

- Regulatory compliance expert in the field
- Written multiple articles on compliance and eDiscovery
- Speaker at 17 Lotus® related conferences/LUGs
- Co-authored two IBM® Redbooks on Linux®
- Designed disclosure response solutions for Fortune® 100, medium-sized, and small established regulated firms

Completing Your Evaluations ...

- Please ensure that you fill-in your session evaluation form
- Thank you in advance

Agenda

- Introduction
- Important Compliance Facets
- Culture and Compliance
- Group Discussion – Implementation
- Compliance Case Corner
- Wrap-up

Why Should You Care?

- eDiscovery requests nearly tripled in 2010
  - Financial Industry Regulatory Authority (FINRA) collected US$50 million in fines in 2009
- 70% of the firms that experience an eDiscovery event go out of business
- Enterprise firms spent approximately US$4.6 billion in 2010 on eDiscovery
- Foreign Corrupt Practices Act (FCPA) enforcement actions jumped 85% (2010)
- Data growth to reach 800% over next five years -- Gartner Group
- **Even if you are not in a regulated industry**, if you have regulated clients or vendors, you could be exposed through their own eDiscovery activities

First-half of 2011 -- Compliance Litigation On The Rise

- "In the first half of 2011, the number and sophistication of e-discovery cases continued to grow at an increasingly fast pace." -- Gibson, Dunn & Crutcher LLP; *2011 Mid-Year E-Discovery Update*

IT Professionals Aren't Saints...

- Many techs should know better and may think they are above the risks of phishing

  But...

  - 50 hackers and 50 IT security professionals fell victim to two fake Facebook profiles from an "attractive 25-year-old female"
  - One of the oldest known tricks still works well; gets a new lease on life in the cyber world

Would you give her your data?
(Actual Facebook profile picture)

The Participants Crumbled

- 78% established trust upon an extended conversation
- 75% revealed details used to guess passwords
  - Phone
  - Address
  - Mother's, Father's name
  - Where they met their partner
  - Other family information
- 94% Security professionals provided the type of password used!
- 83% Hackers provided their password type
  - 13% of security techs and 7% of hackers provided a password example they used or are using

Source White Paper from BitDefender: http://tinyurl.com/dactu338

SOPA and Compliance: The Availability Conundrum

"SOPA would require that Rackspace and other Internet service providers censor their customers with little in the way of due process, trumping the protections present in the current Digital Millennium Copyright Act. What's more, the SOPA bill would seriously disrupt the Domain Name Service that is crucial to the smooth operation of the Web." --Lanham Napier, CEO, Rackspace

- SOPA absolutely deserves monitoring from your legal team and security officers
- If bill passes, plan accordingly
- From a risk perspective, may impact your move to the cloud
- Congress may be backing off; stay tuned...

Source: http://tinyurl.com/7wqubxu

Mandated Disclosure – Keeping IT Interesting

- SEC guidelines on public firms *suggest* that your public firm must disclose all breaches equating “Material impact”
- New guidelines
- Cyberattacks included – “In some cases”
- Determine your exposure to external threats and correlated costs

Source: http://sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm

Federal Requirements for Data Retention

The two most common regulations are missed the most frequently

SOX	5 year minimum for all accounting and audit records	http://www.sec.gov/about/laws.shtml
HIPAA	6 year minimum for all health records	http://www.hhs.gov/ocr/privacy/

Data Retention Needs Can Impact Backup Strategy

- Real-world example
  - Assisted a firm that implemented a backup tape recycle at 60 days, violating SOX
    - They began storing these tapes for five years
  - Discussions around where to store “all these tapes for an additional 58 months — each”
    - Capacity increased from hundreds of tapes to recycle to thousands
  - Quickly exceeded their off-site storage capacity
  - New budget considerations introduced
    - Tape increases
    - New SANs to handle on-site restoration needs
    - Increased monthly off-site storage fees

Capacity Planning, Present State

- 25 tapes per night to handle a backup
- Presuming full backups nightly
- Multiply by 60 days = 1,500 tapes

Capacity Planning, Future State Illustrates Impact

- Growth curve
  - Minimal growth and five years of storage
- Recall that within a five-year window you will have at least one leap year
  - Some industries require seven years

Storage Term	New Tape Count	Differential
Five years	45,650	44,150
Seven years	63,900	62,400

What About Restoration Factor?

- Ensure your capability to pull properly data
  - Any stored backup tape at any time
- Pull random tapes from all archived backups
  - Ensure your system can read the tapes/properly restore files
  - Although tedious, it is absolutely critical to ensure compliance
  - Record any tapes that fail
  - Inform Legal
  - Ascertain your solution/work-around for those data set(s)
  - Plan to prevent the dilemma going forward

A Positive Side-Effect from Compliance

- An effective setup can be utilized to remove doubt or misplace ill will against a colleague

- Real-world example
  - Client asked that I research mail activities for a suspected security breach
  - For the areas of my concern, the Domino environment allowed for unequivocal suspicion removal
  - Result: Person did nothing wrong, but falsely accused

That level of proof is very powerful and ensures that persons of interest avoid any lingering cloud of suspicion that can damage team morale long term

Agenda

- Introduction
- Important Compliance Facets
- Culture and Compliance
- Group Discussion – Implementation
- Compliance Case Corner
- Wrap-up

Setting The Stage...

"Culture eats IT strategy for lunch." –IBM Executive, Oct 2011

Culture Dissection

Two primary types of culture exist in companies:

- End Users
  - Challenges with approach to projects between business and technology
- Intra-technical Team
  - Friends and peers across teams can create unexpected problems later

End Users Driving Technology Decisions

- Seeing all sorts of BYOD setups
- Apple products creating consumer cachet, creating bottom-up adoption
- Media acknowledging the trend
  - Forrester changes aged perspective on Apple in business
  - “Users frequently ignore company rules against the platform.”
  - 41% companies still unofficially support the products, but their users are unrelenting

- Source: http://www.informationweek.com/news/hardware/mac/231901932
- Forrester Report: http://www.forrester.com/rb/Research/people_are_bringing_macs_to_work_%26%238

Can BYOD Work In Your Organization?

- If well managed, having employees and contractors with their own equipment can work in many firms
  - And is currently occurring
- Absolutely need alignment across business leaders, HR, legal, and IT
- If users prefer their own device and use it at work, they give up some freedom
  - Convenience vs. Ownership relationship

BYOD Tips to Help Ensure Success

- Encryption of communication is key to office
  - Native in some apps: Notes®, Traveler®
  - VPN
  - Lotus Mobile Connect® client
- Control Access
- Suggest access agreement/contract
  - Helps IT know who is accessing their network
  - To whom should get access
- Consider multiple profiles -- *dual-persona* apps
  - IT can manage and edit the business one
  - Data mutually exclusive from personal side

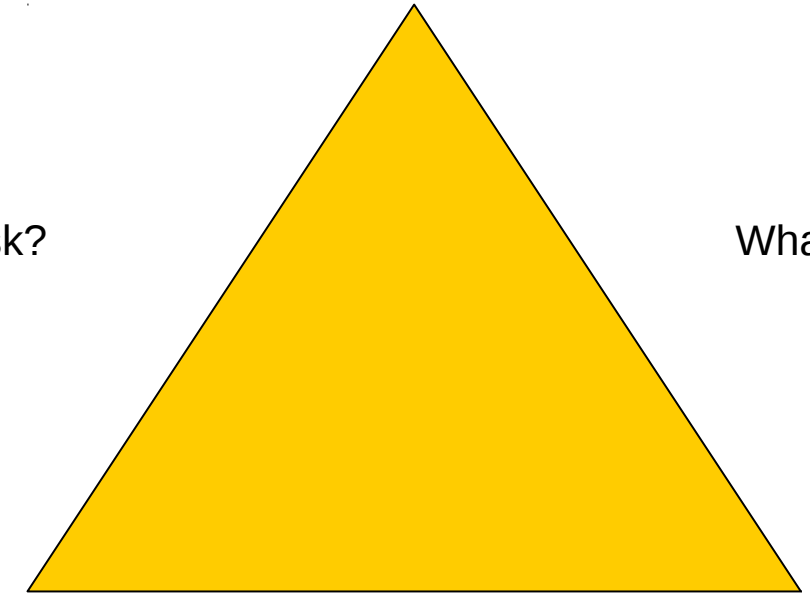
Building Trust With Users Removes A Lot of Headaches

- Users can bypass your policy for several reasons
  - Not always being nefarious
- Avoid policies and procedures that are best for IT
- Reach out to the business line leaders to ensure their business needs are met with technology

Apathy Kills Compliance

- Does this excuse sound familiar?
  - "Courts only request data from companies that have a solution. So, if we do not have an eDiscovery solution, we are safe."
- The current year is not 2000 anymore
- The opposite is true
  - Some courts are willing to provide leniency for eDiscovery costs as burdensome for firms that have robust eDiscovery solutions in-house
  - Source: read in three different eDiscovery journals
  - Note: reiterating this as informational, not a legal opinion

The Regulatory Triangle -- Risk Assessment Guide



The Who
Which firms are at risk?

The What
What data is at risk?

The Why
Which regulations apply to your firm?

Round Up The 'Usual Suspects'

- Investigations typically call upon these four verticals

The Usual Suspects	
Financial	Legal
Accounting	Insurance

- And the rest?
  - Any firm's client can be investigated
  - Courts follow the trail during an investigation
  - Non-regulated verticals can be in-scope if the case warrants such action
    - If your firm is unable or unwilling to respond, life can get interesting very quickly

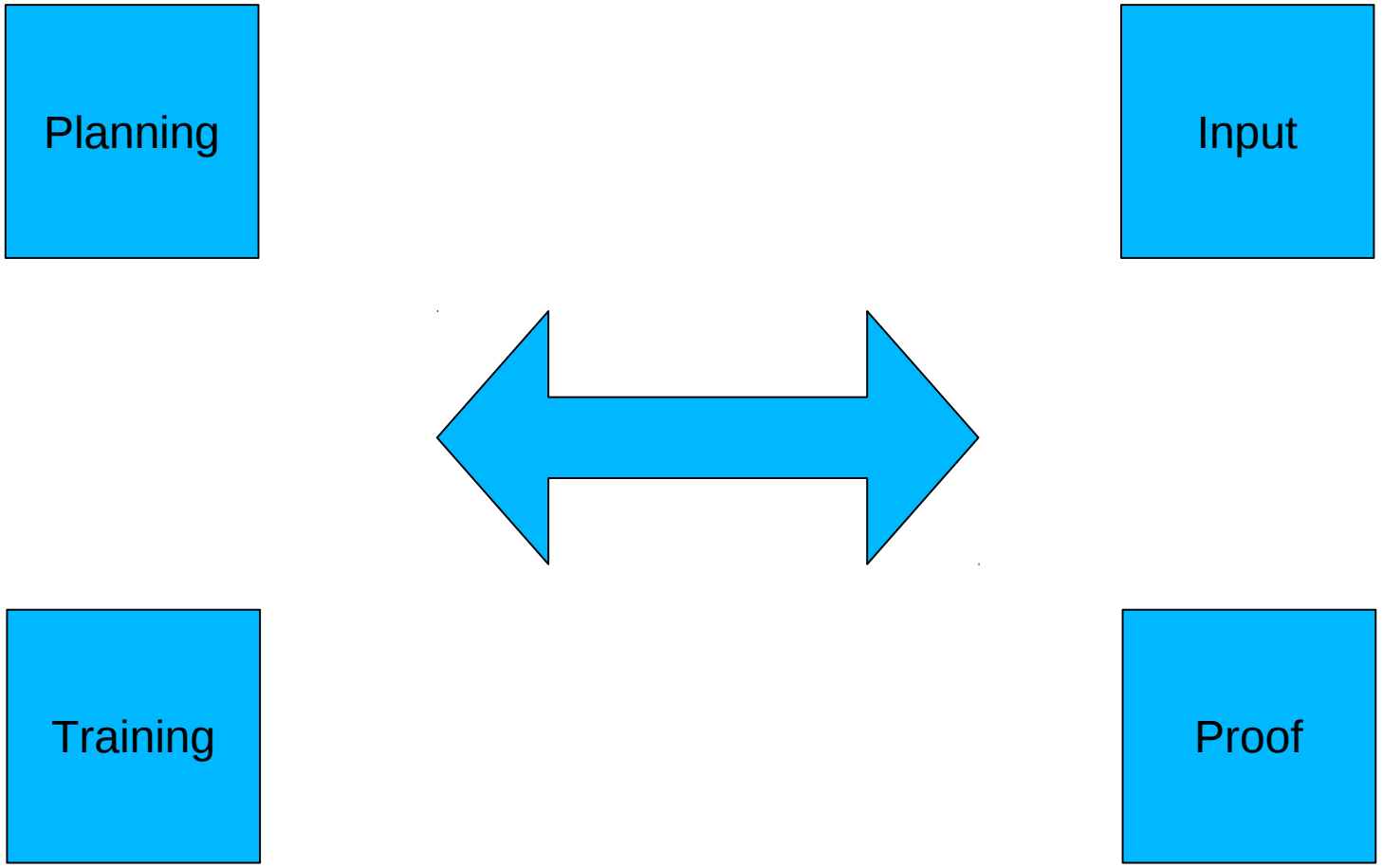
Steps to Protect Yourself

- The best defense is a good offense
  - Although I eschew clichés, it is fitting
- Compliance: much more than e-mail data management

Common Missed Data Sources	
Text messages	Instant messaging data
Calendar events	Mobile equipment

- Protection components
- Message journaling
- Backups
- Full and complete data management strategy

Compliance Success In Four Key Parts



Project and Implementation Plans Are Essential

- Too many teams implement the “Just do it” project execution methodology and hope for the best
  - “We need to get this done,” is quite common
  - *Hope Is Not A Strategy,* by Rick Page
- Planless equates a certain recipe for cost overruns
  - Worst-case is a pending disaster

Get To Know Your Legal Eagles -- It's Mandatory

- Identify your Legal Team liaison
- Ensure your team and legal are present at all meetings
- As new details emerge, decisions can change -- protect yourself
  - Document all decisions agreed upon
  - Version your notes after each change
  - Ensures you are protected and covered
    - Internally and in a court proceeding

Frequent Training Makes Or Breaks The Solution

- Never inform your staff of the policy only once
  - Update routinely
  - One errant task can cost millions
- CIO/CTO's should embrace the K.I.S.S. method
  - Steps to make sure compliance to the company records' retention policy is easy
  - Provides better end-user adherence over what robust and complex offerings yield
  - If it takes more than a few seconds to handle sensitive data, it will be managed improperly/inconsistently
- "We don't do training here," or "We don't need training"
  - Well, Google learned that 90% of users do not know how to use CTRL + F
  - Better rethink that training approach
  - Source: http://tinyurl.com/3nep6rr

Trust But Verify: Managing IT Culture

- Just because you have a drink or watch baseball with other team members...
  - ...Does not mean they will be support you when you need them
- Corporate case-study: Legal response project
  - Performed daily server backups
  - But no restores, till I arrived
  - Why?
    - “Our service level is to backup the servers”
    - “We have no service level for restores”
  - Result: 200k unmarked tapes arrived on-site

Compliance Can Force Data Management Policy

- Motivation is where you find it
  - Failure to provide full information disclosure may introduce significant fines or worse
    - Local laws and infraction severity can vary
  - All infractions land in public domain
  - Negative press can impact your bottom line
    - Significant number of examples of unflattering corporate press impacting stock prices

The Unanticipated Threat...

- Users accidentally or unintentionally sending sensitive data outside of the company
  - SSN & credit card numbers are common
  - Many (new) users do not know what they did is wrong
- Mediums of transport
  - Chat sessions
  - SMS
  - E-mail
  - Social sites and ubiquitous apps

...And The Municipal Legislative Response

- Most states have been active in creating legislation to curb breaches of personal information
- Three styles
  - Media shield prevention -- Companies must report all breaches: most states
  - Require reasonable protections: California, Nevada, Oregon
  - Active monitoring: Massachusetts

Massachusetts	
Name	Massachusetts Standards for the Protection of Personal Information of Residents of the Commonwealth, 201 C.M.R. 17.00
Purpose	"Mandating the development, implementation, maintenance, and monitoring of a 'comprehensive, written information security program'"
Justification	Response from Belmont Savings Bank violation, affected 13,000 residents
URL	http://tinyurl.com/877z5ov

Cybersecurity Threats Are Real and Omnipresent

"According to an FBI study in March 2009, cybercrime — with over $1 trillion in annual revenues — is now the largest illegal global business."

In 2008 Carnegie Mellon CyLab study of 703 board members and senior executives

"Only 36% indicated that their board had any direct involvement with cybersecurity oversight."

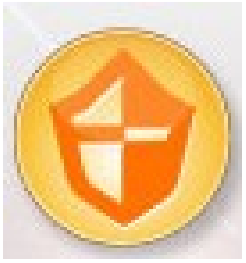
"Not attending to cybersecurity risks could result in enforcement action by the SEC as well as private civil litigation."

Source paper: "Business Leaders Must Address Cybersecurity Risk" by Steven R. Jacobs Esquire and Stephanie L. Chandler Esquire

Source URL: via JD Supra, http://tinyurl.com/73vbbra

One Solution (of Many) – Lotus Protector

- Includes SSN and credit card detectors already included
- Stand alone appliance
- 99.5+% false positive-free filtering
- Highly configurable
- Users get a journal, web access, plus Notes hooks
  - Select message → Add to Protector
    - Automatically creates a new Protector mail rule
    - Avoids the sea of local mail file mail rules
- Runs in a VM or on IBM hardware
- Linux-based, “So you know it’s quality...” :-)



Agenda

- Introduction
- Important Compliance Facets
- Culture and Compliance
- Group Discussion – Implementation
- Compliance Case Corner
- Wrap-up

Security Training for Temporary Workers

- Topic: When and how much training do you offer short-term workers: Is it enough?

- Consideration:

  Balance potential risk versus immediate cost (resource run rate)

Compliance Policy Notifications

- Topic: Knowing one slip-up could incur major fines, how do you keep your users informed of compliance policy changes?

- Considerations:
  - Communication touch points
  - Delivery Medium(s)
  - Frequency / Availability

Agenda

- Introduction
- Important Compliance Facets
- Culture and Compliance
- Group Discussion – Implementation
- Compliance Case Corner
- Wrap-up

Reference Acknowledgement

The cases provided in this section are provided from Information Technology *Adviser*™ and reprinted with permission.

The Case of the Missing Mobile Data

- Business scenario
  - Two employees accused of stealing competitor secrets and put on leave, pending an investigation
  - Lawsuit filed by competitor (Foo, Inc.)
  - Blackberry equipment returned to company
  - Tech purged data on returned devices, as per normal policy
  - IT backed-up all e-mail, but missed text messages, calendar appointments, and call logs
    - Data not archived
  - Suit now includes a charge for intentionally destroying evidence

Who Won The Case?

- Two charges filed:
  - Stealing trade secrets
  - Intentionally destroying evidence

- Decision poll
  - Plaintiff (Foo, Inc.)
  - Defendant (Company)

Arguments

- Plaintiff (Foo, Inc.) argued
  - The defendant cited mobile devices contained data beyond e-mail
    - SMS data
    - Call logs
    - Calendar appointments
    - “Other relevant data” critical to the case
  - This data should have been preserved once the suit was filed
- Defendant argued
  - All e-mails sent via the Blackberries were archived on the corporate server

Court Comments and Verdict

- Statements
  - Judge stated saving e-mails is not enough
  - Company could not provide an adequate response for deleting data before it had been archived
  - Court concluded the company acted in bad faith
    - At the trial, the jury told that the defendant intentionally destroyed evidence
- Decision
  - Foo, Inc. won the suit

Source and Perspective

- E-discovery's scope includes more than e-mail
  - Courts are ruling on smartphones inclusion in e-discovery; be prepared

- Excerpted from Southeastern Mechanical Services, Inc. v. Brody, U.S. District court, M.D. Florida, No. 8:80-CV-1151-T-30EAJ; 31 Aug 2009

Once made aware of impending lawsuit, delete nothing for those in-scope

The Case of the Hacker Who Shared Too Much

- Business scenario
  - Company hacked, sent e-mails being read externally by legal firm negotiating a settlement against the company a year ago
  - Data acquired by hacker provided to legal firm
  - Lawsuit filed by company against the attorney
  - Used the Electronic Communications Privacy Act as basis

Who Won The Case?

- Charge filed:
  - Violated transmission of private data
- Decision poll
  - Plaintiff (Company)
  - Defendant (Attorney)

Arguments

- Plaintiff (Company) argued
  - That they were hacked
  - Showed their data was shared with an attorney it was going against in court
- Defendant argued
  - There was no connection between the hacker and the attorney

Court Comments and Verdict

- Statements
  - Judge threw-out the case
  - Not enough evidence to convict under ECPA
  - Need to show that the attorney conspired with the hacker to convict under the ECPA
  - ECPA only covers the act of hacking into e-mails
    - The hacker rather than the attorney created the breach
    - ECPA doesn’t ban disclosing or using hacked data
- Decision
  - Attorney won the suit

Source and Perspective

- ECPA as a law is myopic
- Companies need to do as much detective work as possible before bringing an electronic breach to court
  - Facts rather than gut instincts or common sense prevail
- Excerpted from Garback v Lossing, U.S. District Court, ED, Michigan, Southern Division, No. 09-cv-12407, 20 Oct 2010

Avoid a situation, rather than go to court; keep your systems' security current

The Case of the Social Site Infringement

- Business scenario
  - Photo taken at company party, posted on Facebook with racially charged commentary
  - Lawsuit filed by victim (Jane Doe)
  - Company now wants to review computer use policy
  - Company took these actions against co-worker (poster)
    - Disciplined policy violator
    - Explained how current policy prohibits co-worker harassment
  - Company monitors employees' activity

Who Won The Case?

- Charge filed:
  - Racial discrimination (through denigratory remarks)
- Decision poll
  - Plaintiff (Jane Doe)
  - Defendant (Company)

Arguments

- Plaintiff (Jane Doe) argued
  - Company is to blame for fostering a hostile work environment
  - Pointed to the Facebook comments as evidence
- Defendant argued
  - We took reasonable precautions
  - Can’t track everything every employee does from every location -- including home

Court Comments and Verdict

- Statements
  - Judge: company not liable for employee's posts
  - Post made on a personal rather than company page
  - Photo at company party is coincidental
  - Co-worker is solely to blame
  - Company could not be expected to know of it immediately
  - The Defendant acted in good faith to resolve situation
- Decision
  - Company won the suit

Source and Perspective

- You are unable to monitor everything and courts realize that
- But, you should be careful to include prose in your technology use policy forbidding co-worker harassment
- Creates an insurance policy to avoid settlements later
- Always follow-up on policy violation matters
- Excerpted from Amira-Jabbar v Travel Services, Inc., U.S. District Court, D. Puerto Rico, No. 08-2408, 28 July 2010

The Case of the Stolen Trade Secrets

- Business scenario
  - Employee left firm, accessed private info
  - Lawsuit filed by company (Foo, Inc.)
  - Customer mentioned that ex-employee visited Foo, Inc.‘s customer
  - Ex-employee still logging-in and accessing company database
  - Ex-employee sought contact data for customers
  - Company safeguards customer data and is concerned

Who Won The Case?

- Charge filed:
  - Stealing trade secrets

- Decision poll
  - Plaintiff (Foo, Inc.)
  - Defendant (John Doe)

Arguments

- Plaintiff (Foo, Inc.) argued
  - They claimed John Doe stole customer info that amounted to trade secrets

- Defendant argued
  - None of the data he accessed was a secret
  - Objected to Foo, Inc.'s definition of a "trade secret"
  - He only acquired basic contact info from the company's data store

Court Comments and Verdict

- Statements
  - Court saw Foo, Inc.’s database --- which they protected with login name and password authentication --- made the data available on a “need-to-know” basis
  - Such preventive actions create the conditions for data being treated as trade secrets
  - Foo, Inc. created a secure environment and thus had the right to protect the data
- Decision
  - Foo, Inc. won the suit

Source and Perspective

- Always safeguard your data
- Keep access lists current; terminate ex-employee's ability to get to data when they leave -- or before they leave
- Protecting data with security measures shows you value it

- Excerpted from Saturn Systems, Inc v Militare, Colorado Court of Appeals, No. 07CA2453, 17 Feb 2011

Best to avoid a situation, before you need to go to court

The Case of the Loss Leasers

- Business scenario
  - Client learns their computer leasing firm sells returned equipment sans a HD wipe
  - Copiers included
  - Systems can contain SSN, internal memos, any and all data
  - Nothing in the contract explicitly stating perform a wipe, nor not to perform a wipe

Who Won The Case?

- Charge filed:
  - Reselling equipment with sensitive data still on it
- Decision poll
  - Plaintiff (Foo, Inc.)
  - Defendant (Equipment vendor)

Arguments

- Plaintiff (Foo, Inc.) argued
  - Claimed the system vendor had a duty to erase any data before reselling
- Defendant argued
  - Appears to allowed the plaintiff to argue for them -- primarily

Court Comments and Verdict

- Statements
  - Court stated it was not the provider's job to keep the company's data safe
  - Its duties only reached to the equipment itself
  - If Foo, Inc. sought to ensure the data would be purged, they should have explicitly written that language into the contract or signed agreement letter
  - Vendor performed within the stated contract and did their job
- Decision
  - Defendant won the suit

Source and Perspective

- Always safeguard your data
- Never assume someone else will do your job f or you
- Good contracts make for good business relationships, avoiding surprises

- Excerpted from Putnam Bank v. Ikon Office Solutions, U.S. District Court, D. Conn., No. 3:10-cv-1067, 7/5/11

Whenever possible, avoid a situation to keep you out of court

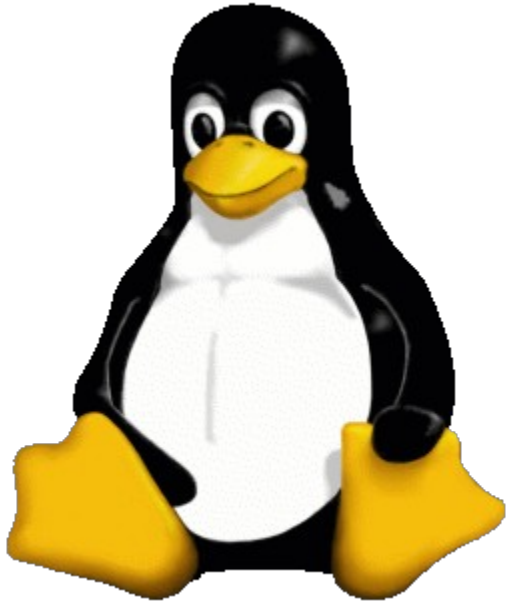
Agenda

- Introduction
- Important Compliance Facets
- Culture and Compliance
- Group Discussion – Implementation
- Compliance Case Corner
- Wrap-up

Resources

- Http://got.good.com/012012BYODW1ConsiderationDoc_byodw1.html
  - "The Bring Your Own Device Policy Consideration Document", Good Technology®
- http://www.ibm.com/developerworks/rational/library/sep05/cancilla-bennet
  - IT Responses to Sarbanes-Oxley
- http://searchdomino.techtarget.com/generic/0,295582,sid4_gci1321695,00.html
  - IT Governance in an IBM Lotus Software Environment
- http://searchdomino.techtarget.com/news/article/0,289142,sid4_gci1222736,00.h
  - IM, Blogs Next Target for Litigation

Just Approved!



Linuxfest Returns to Lotusphere!

By Popular Demand, Linuxfest is at LS12

What: *Linuxfest* III

When: Thursday, 19 Jan

Where: **Dolphin, Europe 6**

Time: 12:30 - 1:30 pm

Other: Bring your box lunch!

We're not in the program guide, so mark your calendar

THANK YOU!

Any Questions?

Contact Information

Bill Malchisky Jr.

IBM CHAMPION

- E-mail: bill@billmal.com
- Skype: fairtaxbill
- Twitter: billmalchisky

- My Website: http://www.effectivesoftware.com
- My Blog: http://www.BillMal.com