

Regulatory Enforcement: A Shifting Threat Model

Brandon Dunlap
Director of Research

Mark Adams
Senior Researcher

Agenda



- Who are we and what is Brightfly?
- Predicting Impact
- Enforcement Trends
- Trends in IT Controls Selection
- Q&A

What We Do




- Brightfly
- Community-based “open source” analyst firm
- Bridges the gaps between vendors, consultants, and you
- Includes the financial community


Predicting Impact

Who has a crystal ball?

"The Black Swan"



- We place too much weight on the odds that past events will repeat.
- The really important events are rare and unpredictable.



10827 Oasis Drive Houston, TX 77096 p. 877.885.8507

Copyright © 2007 Brightfly All Rights Reserved

Gauging a potential employee's temperament – easier under severe circumstances; law enforcement knows this (interrogations)

9/11 attacks

Stock market crash of 1987

SOX?

Use Cardsystems example. They blamed their auditors and consultants. The settlement requires Pay by Touch to implement a comprehensive security program and obtain independent audits every other year for 20 years (deferred prosecution).

almost all consequential events in history come from the unexpected—while humans convince themselves that these events are explainable in [hindsight](#).

Bell curve ignores large deviations b/c it cannot handle them

Single Loss Expectancy (SLE)



- We try to estimate the impact of a single incident or event
 - But can we really predict costs associated with things like legal fees, forensic investigations, and restitution?



What about punitive damages? Notification? Cleanup?

Predicting Impact Is Virtually Impossible




- Fines and penalties can be known to a degree...

...however, what would the TRUE cost be should a breach occur?

Example: Penalties for non-compliance with PCI can range from fines of up to \$500,000 to increased auditing requirements or even losing the ability to process credit card transactions.

Case In Point: TJX



- Visa levied an “egregious fine” of \$500K due to the seriousness of the breach
- Visa added another \$380K for failure to stop storing sensitive data
 - Total (so far): **\$880,000**
- In addition, Visa said it would continue assessing fines of up to \$100,000 per month until TJX becomes compliant

10827 Oasis Drive Houston, TX 77096 p. 877.885.8507

Copyright © 2007 Brightfly All Rights Reserved

The fines were levied against Fifth Third, TJX’s acquirer, but the assumption is these fines will be passed through to TJX.


TJX increased its estimate of pre-tax charges for the world's worst credit card data breach to \$216 million. Back in August, it had projected only a \$168 million pre-tax hit.

"This reserve reflects [TJX's] estimation of probable losses in accordance with generally accepted accounting principles based on information available to [TJX] and includes an estimation of total potential cash liabilities, from pending litigation, proceedings, investigations and other claims, as well as legal and other costs and expenses, arising from the computer intrusion," TJX said in its SEC filing.


Who wants to be the one to tell the BoD why the estimates were wrong?

Enforcement Trends

Who Do You Need to Worry About?



SOX



- Organizations are continuing to adjust to SOX
 - Reduced number of controls
 - Optimizing and streamlining controls
 - Balancing traditional audit responsibilities with compliance activities

...but, smaller companies now have to comply!

10827 Oasis Drive Houston, TX 77096 p. 877.885.8507

Copyright © 2007 Brightfly All Rights Reserved

Audit fees are falling for SOX work; however, smaller companies now have to comply

HIPAA enforced by Office of Civil Rights

Payment Card Industry (PCI)



- In 2006, Visa levied \$4.6 million in fines, up from a 2005 total of \$3.4 million.
- The PCI Security Standards Council anticipates expanding requirements next year.
- Payment Application Data Security Standard (PA-DSS) released on November 7th.

New requirements will probably relate to wireless use as well as web application security.

There's considerable debate going on as to what the new requirements will be so we'll just have to wait and see.

Federal Trade Commission


Enlighten Your Enterprise

- The most active and aggressive of all the U.S. government regulatory oversight agencies in going after noncompliant organizations.
 - Those that are practicing "unfair and deceptive trade practices."

10827 Oasis Drive Houston, TX 77096 p. 877.885.8507

Copyright © 2007 Brightfly All Rights Reserved

ChoicePoint was used as an example; Majoras pointed out the company had violated Section 5 of the Federal Trade Commission (FTC) Act, which prohibits unfair or deceptive trade practices, and they also violated the Fair Credit Reporting Act. Section 5 of the FTC Act provides for sanctions to be applied in the form of consent orders, such as detailed activities that must be performed for typically 20 years, but it does not allow for the imposition of fines. So, the FCRA charge was the basis on which the court approved the \$10 million fine (in January 2006) against ChoicePoint.

The violation was not the data breach, but the **non-existence of appropriate security** that would have prevented the breach.

Currently has more than 24 open information security investigations going on.


The FTC's "Hall of Shame"


10827 Oasis Drive Houston, TX 77096 p. 877.885.8507

Copyright © 2007 Brightfly All Rights Reserved

ChoicePoint was fined \$15m over a data security breach that led to at least 800 cases of identity theft. ChoicePoint agreed to pay \$10m in civil penalties (a record fine) and \$5m to compensate consumers.

- U.S. financial organizations, and ANY company that possesses information about U.S. customers with which identity theft could occur, are now **legally required** to have a documented Identity Theft Prevention Program
- Final rules issued on October 31st of this year.

eDiscovery

BRIGHTFLY
Enlighten Your Enterprise

- UBS Securities fined \$2.1 million for failure to preserve email
- Morgan Stanley fined \$12.5 million for mishandled email

10827 Oasis Drive Houston, TX 77096 p. 877.885.8507

Copyright © 2007 Brightfly All Rights Reserved

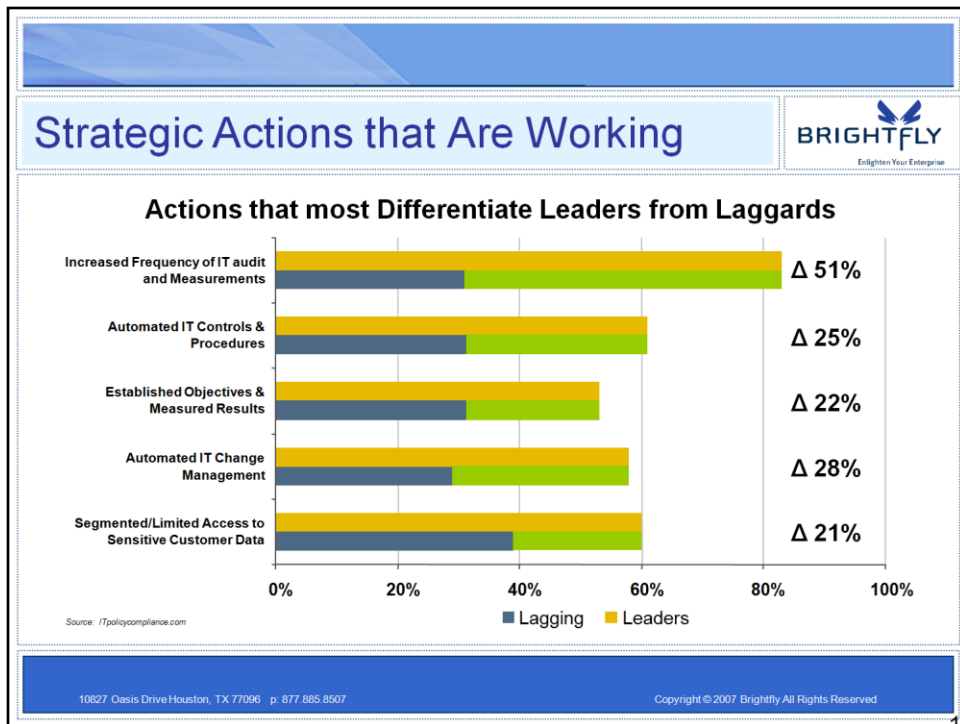
According to a recent study by [The Radicati Group](#), in 2007 a typical corporate account will generate around 4.3 gigabytes (GB) of electronic data per user. That number is expected to grow to 6.7 GB per year by 2011.

Keep an eye on NERC. Readiness audits taking place in 2007, so let's wait and see what happens in 2008.

- NERC
- Japan SOX (“J-SOX”)
- International Financial Reporting Standards (IFRS)

Trends in IT Controls

What Is Everyone Else Doing?

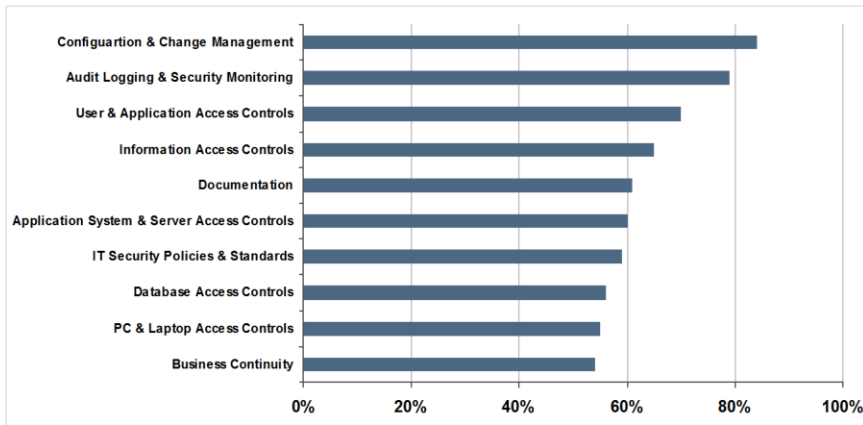


- We've done research across 1000s of organizations of all sizes to see what most correlates to being a leader vs. laggard (as defined by # of significant deficiencies).
- Far and away, the most highly correlated action is "Frequency of Internal audit". That's not surprising... practice makes perfect. And the more internal audits you do the more aware you will be about your deficiencies, and you can take steps to remediate them. There are other top correlated actions as well.

Top 5:

1. Increased frequency of audit [all of CCS]
2. Automated IT controls and processes [Standards, Entitlements and Response Assessment module]
3. Establishing objectives and measuring results [Policy and Standards module]
4. Automated IT management [Standards module]
5. Limit access to sensitive data [Entitlement module]

Which IT Controls Are Most Deficient?



Source: [ITpolicycompliance.com](http://policycompliance.com)

Identity and Access Management



- 3 out of the 5 top internal audit findings are related to identity and access management
 - Excess access rights
 - Lack of audit trails/logging
 - Access control compliance with procedures
- On average, 17 accounts are created for an individual during his tenure, but only 10 are removed when he leaves

-- Source: 2007 Deloitte Global Security Survey

Top Management Must Take Ownership



“Even though information security incidents are grabbing the attention of business executives and boards, these individuals do not yet feel that they *own* the problem; in their estimation, the execution of solutions are the mandate of IT.”

-- Source: 2007 Deloitte Global Security Survey

Leaders Manage the Threat



- Leading organizations treat the compliance process less like a project and more like any other risk factor
- Leaders use governance to guide and improve performance
- Leaders have executives and BoDs that take ownership of the problem

Q&A



- What have been your experiences?
- Challenges?
- Success stories?

Additional Resources



- www.brightfly.com
- www.itpolicycompliance.com
- www.itcinstitute.com
- www.itgi.org
- www.isaca.org


Thank you



Brandon Dunlap
Director of Research
bsdunlap@brightfly.com

Mark Adams
Senior Researcher
mradsams@brightfly.com

Brightfly, Inc.



BREAK

10827 Oasis Drive Houston, TX 77096 p. 877.885.8507

Copyright © 2007 Brightfly All Rights Reserved

Agenda



- Who are we and what is Brightfly?
- Intro to Risk Management
- Common Pitfalls in Risk Management
- Baking It In
- Q&A

What We Do



- Brightfly
- Community-based “open source” analyst firm
- Bridges the gaps between vendors, consultants, and you
- Includes the financial community

Risk Management

Science or Art?

High Speed History Lesson



Enlighten Your Enterprise

“More than any other development, the quantification of risk defines the boundary between modern times and the rest of history.”

Peter L. Bernstein, *Harvard Business Review*, Mar.-Apr. 1996, p. 57-51.

Basic Games of Chance



Early dice made from sheep bones

Renaissance Studies on Probability



Galileo publishes "Sopra le Scoperte" in 1630

The Birth of Insurance



Lloyd's of London circa 1774

10827 Oasis Drive Houston, TX 77096 p. 877.885.8507

Copyright © 2007 Brightfly All Rights Reserved

- In his 1998 book *Against the Odds*, Peter Bernstein describes how thinking about risk evolved in part because of changes in mathematical numbering systems, an understanding of the statistical basis of probability, and the rise in popularity of gambling.
- Although games of chance and gambling were depicted in Egyptian tomb paintings from 3500 B.C.E., it wasn't until the Renaissance that a "scientific" or statistical basis for gambling was presented.
- Girolamo Cardano, a sixteenth-century physician, gambler, and mathematician wrote *Liber de Ludo Aleae* ("Book on Games of Chance") perhaps the first study of probability in cards, dice throwing, and gambling.
- "Sopra le Scoperte" ("On Playing Dice") published in part for Cosimo II de Medici, the Grand Duke of Tuscany, whom Galileo had tutored in math. Cosimo II, ironically, upon taking power closed the Medici bank and swore off commercial activities as "degrading for a prince".
- Lloyd's of London was born in a coffee shop, owned by Edward Lloyd, near the Tower of London in 1687, in part because the shop was a gathering place for ship captains who shared news about past and upcoming voyages, trade routes, weather, and hazards. Those who wanted to share in a risk could sign their names on a board under the terms of a contract that all could see.
 - From this practice arose the term "underwriters."
 - Like having your boss sign off on a risk acceptance form, eh?

Measuring Risk is *Hard*



We've reduced this...

$$\begin{aligned}(1 - L)^d X(t) &= \sum_{\tau=0}^{\infty} \left[(-1)^\tau \binom{d}{\tau} \right] L^\tau X(t) \\ &= \sum_{\tau=0}^{\infty} a(\tau) X(t - \tau) \\ &= \varepsilon(t), \text{ with } \varepsilon(t) \sim i.i.d.(0, \sigma_\varepsilon^2)\end{aligned}$$

...to this.

$$(ARO)(SLE) = ALE$$

10827 Oasis Drive Houston, TX 77096 p. 877.885.8507


Copyright © 2007 Brightfly All Rights Reserved

- Equation from paper on financial risk modeling over time (<http://129.3.20.41/eps/fin/papers/0502/0502013.pdf>)
- Despite fantastic mathematical leaps in the quantification of financial risk, we have been woefully inadequate in applying the same discipline to Information Security risks.

$$\begin{array}{c} \text{(Annualized Rate of Occurrence)} \\ \times \\ \text{(Single Loss Expectancy)} \\ = \\ \text{Annual Loss Expectancy} \end{array}$$

Example

(Annualized Rate of Occurrence)	50%
X	X
(Single Loss Expectancy)	\$500,000
=	=
Annual Loss Expectancy	\$250,000


BRIGHTFLY
Enlighten Your Enterprise

10827 Oasis Drive Houston, TX 77096 p. 877.885.8507

Copyright © 2007 Brightfly All Rights Reserved

Modern compliance management is like playing dice with oblong knuckle bones.

You Cannot Predict Misfortune



- You do not *know* what the Average Rate of Occurrence is.
- Your *best* hope is to pull a plausible average out of the air

10827 Oasis Drive Houston, TX 77096 p. 877.885.8507

Copyright © 2007 Brightfly All Rights Reserved

- You don't know what the odds are that you will get exploited on a given vulnerability, or that an employee laptop will "grow legs", or any other risk for that matter.
- Many low-probability events are the highest impact.



- ChoicePoint's stock dropped 15% on the news of exposing 162,000 people's personal information to fraudulent access.
- Share volume was 3-6 times the average after the announcement.
- That 15% represented **\$630 million of shareholder wealth.**
- Aug. 23rd: SBA Survey finds that the average employer with 20 employees pays about **\$7, 647 per employee** in regulatory costs (\$1,304 of this is tax compliance). The average cost per employee for large firms is about **\$5,282.**
- Aug. 16th: In a filing with the Securities & Exchange Commission, TJX Companies stated its estimated cost for the computer intrusions it disclosed earlier this year has now reached a total of **US\$118 million.**
- Sept. 3rd: Monster reports a breach that exposed **1.3 million resumes.**
- Sept. 6th: Pfizer reports 3rd breach since June, latest incident involves **34,000 employee records.**

It Isn't All Doom and Gloom



- We aren't here to say it's hopeless.
- We will show you methods and practices to make it more palatable...
- ...and a lot more practical.

- And we'll tell you about our mistakes so that you can learn from them.

Risk Management Pitfalls

Make New and Exciting Mistakes

Pitfalls



Lack of Accountability

- No one is ultimately responsible for driving the process to successful completion.

Strategy

- Obtain support and involvement from senior management
- Designate a project / program manager
- Define project management procedures
 - Roles / responsibilities, etc.
- Make it **VISIBLE**

Pitfalls (continued)



Lack of participation

- The relevant parties are not coming together to participate in the assessment process

Strategy

- Involve stakeholders from relevant organizations
 - Technical and Business
- Enforce accountability
- Document, maintain, and compare / analyze results

Pitfalls (continued)



Project Stalls

- The assessment process/project loses steam.


Strategy

- Redefine / limit the scope
- Ramp up risk management awareness efforts to drive visibility

Establishing a Risk Management Program

"Baking It In"

Choose a Controls Framework



- ISO17799
- ISO27000 Series (replaces ISO17799)
- NIST SP800 series
- COBIT
- ITIL
- How many of you have a “favorite” framework?

10827 Oasis Drive Houston, TX 77096 p. 877.885.8507
Copyright © 2007 Brightfly All Rights Reserved

- Cobit
 - First edition was released by ISACA in 1996
 - Second edition in 1998
 - Third in 2000
 - Fourth in 2005!
 - 5 years between updates!
- ISO
 - Originally published as DTI code of Practice for Information Security in the early 90's
 - Became ISO standard in December 2000
 - Last updated in 2005
 - 5 years between updates?!?!?
- ITIL
 - Originally authored in the 1980's by the UK's Central Computer and Telecommunications Agency

Cost-Benefit Analysis



- Determine which controls are required and appropriate for the circumstances
- Demonstrate that the costs of implementing the controls can be justified by the reduction in the level of risk
 - Qualitative / Quantitative
 - Determine the impact of implementing the new or enhanced controls
 - Determine the impact of *not* implementing the new or enhanced controls
 - Estimate the cost of the implementation
 - Assess benefits against security posture

Getting buy-in



- HR
- Legal
- IT
- Finance
- Who else?

Staying On Track



- You cannot manage what you cannot measure
- Key Performance Indicators
 - % critical assets/functions residing on compliant systems
 - % critical assets/functions with documented risk assessments/profiles
 - % critical assets/functions reviewed for physical security/risk
 - % critical assets/functions with documented risk mitigation plans
 - % critical assets/functions with documented "cost of compromise" estimate

What gets measured gets improved.

Measuring Success Through Competition



- **Internal**

- Team vs. Team
- Department vs. Department

- **External**

- Across industry peers
- Industry vs. Industry
- Geographically
- Demographically

Driving Organizational Behavior



- Awareness of risks leads people to alter their decision-making behavior
- The key is not to eliminate risk, but to manage around it.
 - Be careful of creating a risk averse culture!

Leaders vs. Laggards



Leaders

- Choose a framework and stick to it
- Assign accountability for the program
- Focus on the process, not the technology
- Buy tools to support the process, not the outcome

Laggards

- Follow "trends" and "fads", hopping from one approach to another
- Manage by committee
- Drive for more capital spend rather than leveraging existing tools
- Focus on point solutions rather than more holistic approaches.

Thank you



Brandon Dunlap
Director of Research
bsdunlap@brightfly.com

Mark Adams
Senior Researcher
mradsams@brightfly.com

Brightfly, Inc.