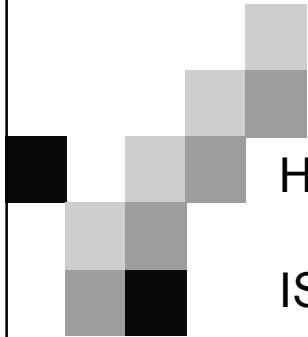


SBO



Hidden Causes of Data Loss

ISACA March 12, 2009

Dave Morrow
President
Secure Business Operations, LLC

SBO

Overview

- “Hidden” loss as a business risk
- Causes
- Lessening the risk

SBO

“Hidden” loss is a silent risk

- 90% of breaches in 2008 Verizon Data Breach Report involved:
 - Data the victim didn't know it had
 - A system/process not known to the victim
 - A known system with unknown network connections
 - A system with unknown accounts or privileges

Source: 2008 Verizon Data Breach Report

SBO

Failure to monitor outsourcers/partners

- Many companies have outsourced key business functions with little thought to the outsourcer's security capabilities and practices
- Subcontractors were responsible for **45%** of the total number of records reported lost in 2008
(Source: Identity Theft Resource Center 2008 Data Breach Report)
- Many companies are unaware of what data the outsourcer maintains
- You may still be held accountable if your vendor loses sensitive personal data

SBO

Poor media storage practices

- Portable media can be a treasure-trove of sensitive data – one tape or disk can hold millions of records
- Large data centers can contain hundreds of thousands of tapes and disks
- Accountability and inventory is sometimes poor to non-existent
- Off-site storage offers additional accountability problems
- Transporting media is a particular vulnerability

SBO

Poor or antiquated business processes

- Years-old business processes have remained substantially unchanged
- Often such processes exist in organizations where IT is decentralized
- Some instances of sharing sensitive data are obvious; others not nearly so
 - Sharing health data with insurers, sampling data for audits, benefits consultants, etc
 - Moving data between the company and other 3rd parties for travel, HR benefits, mergers and acquisitions, etc

SBO

Careless handling of 'hidden' sensitive data

- Often sensitive data is “hidden in plain sight”
 - Example: SSAN masquerading as a “customer number”
- Applications using personal data as identifiers are particularly vulnerable
- Downsizing could increase the risk here

SBO

Lack of recognition of data the organization holds

- 66% of breaches involved data the victim didn't know they had (source: Verizon 2008 Data Breach Investigations Report)
- IT (and thus IT security) is assumed to know but many times doesn't
- Decentralization of IT function into business units aggravates the problem here also

SBO

“Inheriting” risk through acquisition

- Most companies do a great deal of due diligence
 - Few include information security in their due diligence.
- Routine due diligence will seldom disclose risk from data loss incidents that have occurred
 - Fewer will uncover a loss waiting to occur
- Sometimes incidents evolve from minor to major over time as investigations disclose more loss
 - A seemingly minor loss can balloon into a major one

SBO

Lack of a “security culture”

- Most companies have security awareness programs
 - Some also include specific training on sensitive data responsibilities for selected employees
 - Few outside this group can reliably identify sensitive data
- Awareness programs sometimes merely “checking the box”

SBO

How to lessen your risk (People)

- Work towards a “culture of security”
 - Messaging should be frequent, varied, and tested
- Awareness should involve the entire organization
 - Support units may be most vulnerable to hidden loss scenarios
 - HR, Logistics, Contracting, Audit all should have awareness of the threats

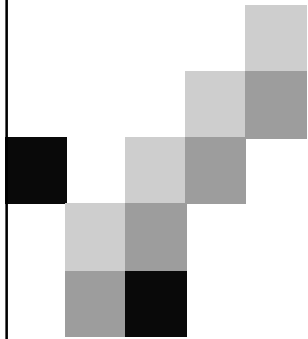
SBO

How to lessen your risk (Process)

- Security practices should be an integral part of:
 - M&A, partnering and outsourcing due diligence
 - Contracting process and administration
- Clearly identify sensitive data and how and where it moves around the organization
- Think holistically about how data exists – some of the biggest incidents have involved paper

How to lessen your risk (Technology)

- Guard against the “silver bullet” bias towards technology in management and employees
- Install some sort of data leakage discovery/prevention tool (you’ll be surprised at the findings!)
- Demand vendors and partners use available technology (example: electronic data transfer vs tapes and paper)



Comments?

Dave Morrow
214-724-4604
davemorrow@securebusinessoperations.net
www.securebusinessoperations.net