


Welcome

**Information Security
And Data Handling For
E-Commerce Businesses**

**Presented by:
Norman Katz, Katzscan Inc.**


Copyright © 2008 – Katzscan Inc. Information Security And Data Handling For E-Commerce Businesses



About The Presenter

- Norman Katz, owner & founder
- BSBA & Computer Science – UF – 1985
- Katzscan founded January 1, 1996
- Florida Private Investigator – 1998
- Certified Fraud Examiner – 2006
- Corporate Governance Cert. – 2007
- Certified Fraud Specialist – 2008


Copyright © 2008 – Katzscan Inc. Information Security And Data Handling For E-Commerce Businesses



About Katzscan

- Barcode Applications
- Electronic Data Interchange (EDI)
- Supply Chain Vendor Compliance (↑ & ↓)
- Software Selection & Implementation
- Data Reporting / Analysis / Conversions
- Database Design / Software Development
- ERP Systems & Business Operations
- Supply Chain Fraud & Governance


Copyright © 2008 – Katzscan Inc. Information Security And Data Handling For E-Commerce Businesses



Presentation Outline

- Risk Management
- Key Data Collected
- Data Verification & Validation
- Data Handling
- Physical Security
- Competitive Intelligence

Copyright © 2008 – Katzscan Inc. Information Security And Data Handling For E-Commerce Businesses




Risk Management

Characteristics Of A Risk:

- Frequency
- Severity
- Likelihood

Example: Hurricane Season

Copyright © 2008 – Katzscan Inc. Information Security And Data Handling For E-Commerce Businesses



Proactive Risk Management

Catch small risks before they turn into big problems

- Easier to manage
- More affordable to address
- Identify before “manifestation”
- Less repercussions to deal with

Copyright © 2008 – Katzscan Inc. Information Security And Data Handling For E-Commerce Businesses



Protect Your Business

Minimize business decisions or transactions based on bad data.

Copyright © 2008 – Katzscan Inc.
Slide 7

Information Security And Data Handling For
E-Commerce Businesses

katzscan.

Key Data Collected

- Customer ship-to address & phone
- Customer bill-to address & phone
- Customer e-mail address
- Customer payment information
- Products ordered & prices paid

Copyright © 2008 – Katzscan Inc.
Slide 8

Information Security And Data Handling For
E-Commerce Businesses

katzscan.

Validate & Verify

- Validation
 - Is the data “good”?
 - Does the data make sense?
 - Is the data within acceptable parameters?
- Verification
 - Can the data be checked against a trusted source?

Copyright © 2008 – Katzscan Inc.
Slide 9

Information Security And Data Handling For
E-Commerce Businesses

katzscan.

Is The Data “Good”?

- Use drop-down lists whenever possible
 - State (Tip: Use name, not code)
- Comparative Checks
 - Zip Code to city & state
 - Area Code to city & state or Zip Code
- Field edits
 - Numeric versus Alphanumeric entries
 - Minimum & Maximum field lengths

Copyright © 2008 – Katzscan Inc.
Slide 10

Information Security And Data Handling For
E-Commerce Businesses

katzscan.

Does The Data Make Sense?

- Phone numbers with “555” prefix
- Too many consonants or vowels in series
- Names that contain numbers or words
- Special characters in fields * \$ # @ !
 - SQL Injection is a common hacking trick!
- Make error messages clear to customer
- Lower costs by mitigating the help call

Copyright © 2008 – Katzscan Inc.
Slide 11

Information Security And Data Handling For
E-Commerce Businesses

katzscan.

Is The Data Acceptable?

- Bill-To and Ship-To addresses in different states for same name
 - Is this a gift or is this fraud?
- Orders of excessive quantity of items
- Orders with excessive line items
- Not-for-export items
- Items with state or age restrictions
- Shipments to a post office box

Copyright © 2008 – Katzscan Inc.
Slide 12

Information Security And Data Handling For
E-Commerce Businesses

katzscan.

Has The Data Been Verified?

- USPS address verification
 - Bill-To address
 - Ship-To address
- Credit card bill-to name and address
 - Phone number too?
- Birth month & year for restricted items
 - Verify with credit card processor?
 - Force telephone ordering only?

Copyright © 2008 – Katzscan Inc. Information Security And Data Handling For E-Commerce Businesses



Data Handling

Chain Of Custody

- “Who had what?”
- “When did they have it?”
- “Why did they have it?”

Copyright © 2008 – Katzscan Inc. Information Security And Data Handling For E-Commerce Businesses



Chain Of Custody Factors

- Was data necessary for job role?
- Was there an approval process?
- How accessible was the data?
- Were there safety & security policies?
 - Especially to take data off-premises
- Check-In / Check-Out log?
- Knowledge of what data was accessed?

Copyright © 2008 – Katzscan Inc. Information Security And Data Handling For E-Commerce Businesses



Why Policies Are Important

United States Sentencing Guidelines

www.ussc.gov

Copyright © 2008 – Katzscan Inc. Information Security And Data Handling For E-Commerce Businesses



Sentencing Reform Act of 1984

1. Setting of base fine
 - Table of 43 base fines
 - Gain or Loss factor
2. Multipliers based on:
 - History & Tolerance of criminal activity
 - Self-reporting, cooperation, guilt acceptance
 - Obstruction of justice
 - Policies and programs in place

Copyright © 2008 – Katzscan Inc. Information Security And Data Handling For E-Commerce Businesses



Security

- Physically
- Accessibility
- Readability
- Usability

Copyright © 2008 – Katzscan Inc. Information Security And Data Handling For E-Commerce Businesses



Physical Security

- Building structure
- Room access
- File cabinet access

- Use of locks and pass-cards
- Recording of physical access
 - User / Date / Time / Location
 - Cameras

Copyright © 2008 – Katzscan Inc. Information Security And Data Handling For E-Commerce Businesses **katzscan.**

Accessibility

Who has access to what based on job role?

- Copy machine
- Computer software
- Network
- File folders
- Documents (physical & electronic)

Tie to HR job description

Copyright © 2008 – Katzscan Inc. Information Security And Data Handling For E-Commerce Businesses **katzscan.**

Readability

Encryption of data

- Third-party encryption tools
- In-house encryption “recipe”

Copyright © 2008 – Katzscan Inc. Information Security And Data Handling For E-Commerce Businesses **katzscan.**

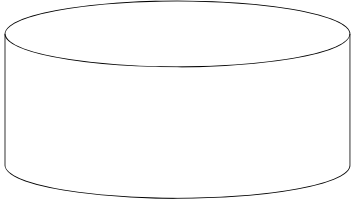
Usability

Can data be fragmented to “unusable” silos of information?

- Name & Address
- Credit Card Number
- CC Expiration Date
- Product History

Copyright © 2008 – Katzscan Inc. Information Security And Data Handling For E-Commerce Businesses **katzscan.**

Data Silo – Example 1




Complete customer record (name, address, CC, order history, etc.)


Copyright © 2008 – Katzscan Inc. Information Security And Data Handling For E-Commerce Businesses **katzscan.**

Data Silos – Example 2


Name & Address




Credit Card Number




Account Key



CC Expiration & ID



Product History




Arrows indicate relationships between the silos.

Copyright © 2008 – Katzscan Inc. Information Security And Data Handling For E-Commerce Businesses **katzscan.**


Data Silos – Example 3

Name & Address




A

Credit Card Number




C

Account Key Reference




CC Expiration & ID



B

Product History



D

12345 – A – Table ID
 12345 – B – Table ID
 12345 – C – Table ID
 12345 – D – Table ID

Copyright © 2008 – Katzscan Inc. Information Security And Data Handling For E-Commerce Businesses **katzscan**

Data Camouflage

- Introduction of purposefully junk data
- Use of non-descript table names
- Altering sort order in different tables
 - If all tables are in “entry” order, silo data can be matched on record number
- Variation of encryption routine by table
 - Encrypt data record's date/time stamp to minimize cross-table matching

Copyright © 2008 – Katzscan Inc. Information Security And Data Handling For E-Commerce Businesses **katzscan**

Competitive Intelligence

Society of Competitive Intelligence Professionals

www.scip.org

Copyright © 2008 – Katzscan Inc. Information Security And Data Handling For E-Commerce Businesses **katzscan**

When Innocuous Data Isn't

How could a person use your company's intellectual information to cause you harm or damage?

- Hack Attack
- Disgruntled Employee
- Competitor

Copyright © 2008 – Katzscan Inc. Information Security And Data Handling For E-Commerce Businesses **katzscan**

C.I. Example

What does your grocer know about you?

- Family Size
- Schedule / Habit
- Life Style
- Income Level
- Allergies / Health Issues
- Gender

Copyright © 2008 – Katzscan Inc. Information Security And Data Handling For E-Commerce Businesses **katzscan**

PCI DSS

Payment Card Industry Data Security Standards

www.pcisecuritystandards.org

Copyright © 2008 – Katzscan Inc. Information Security And Data Handling For E-Commerce Businesses **katzscan**

PCI Highlights

- Secure Network
 - Firewalls and Anti-Virus software
- Encrypt data in transit
- Application Security
- Data Access Restrictions
- Monitor & Test Security Measures
- Maintain Information Security Policies

Copyright © 2008 – Katzscan Inc.
Slide 31

Information Security And Data Handling For
E-Commerce Businesses



Summary

- Data security is internal & external
 - Infrastructure & Information
- Think like law enforcement
- Document policies and procedures
 - Enforce them too!
- Proactive Risk Management

Copyright © 2008 – Katzscan Inc.
Slide 32

Information Security And Data Handling For
E-Commerce Businesses



Thank You!

Any Questions?

www.katzscan.com

Copyright © 2008 – Katzscan Inc.
Slide 33

Information Security And Data Handling For
E-Commerce Businesses

