

Willing to Risk Your Reputation?

What's In Your IT Policy?

**Presented by: Jim Soenksen, CEO
Pivot Group, LLC**



HIGH FIVE
Don't bet
against him p. 11

CHILD PORN
Crackdown
on creep p. 18

GOOGLE EARTH
Beyond the fun
factor p. 28

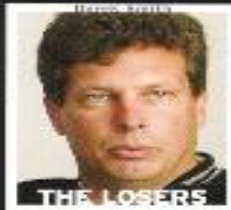
TECH GUIDE
Douse the
mouse p. 35

CAREERS
Project managers
in demand p. 39

InformationWeek

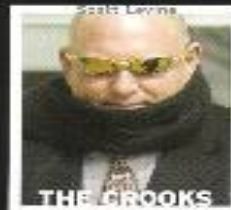
MARCH 20, 2006

BUSINESS INNOVATION POWERED BY TECHNOLOGY



THE LOSERS

Businesses continue to handle personal data with alarming ineptitude.



THE CROOKS

SORRY STATE OF AFFAIRS



THE VICTIMS

Here's the ugly truth about how it keeps happening—and the costly ramifications.

P. 34



THE LAW

ISSN 1545-8933

0000-0000-0000-0000

0000-0000-0000-0000

0000-0000-0000-0000

0000-0000-0000-0000

0000-0000-0000-0000

0000-0000-0000-0000

0000-0000-0000-0000

0000-0000-0000-0000

0000-0000-0000-0000

0000-0000-0000-0000

0000-0000-0000-0000

0000-0000-0000-0000

0000-0000-0000-0000

0000-0000-0000-0000

0000-0000-0000-0000

SUITE-NER Bill Gates talks up the overhaul of Office p. 33

Agenda

- What is a Policy?
- Why are Policies Important?
- What is the DNA of a Quality Policy?
- Are Policies Enough?
- Key Policies & Procedures & Controls
- Policy Development & Implementation
- How do You Know You have Succeeded

It looks like a Policy!

- Webster: A definite course of action for the sake of expediency, facility, or the like
- SANS: A document that outlines specific requirements or rules that must be met
- NCUA: You must have!

Why a Good IT Policy?

- Link to Business Strategy
- Regulatory Compliance
- Define Appropriate Behavior
- Define Tools & Procedures
- Consistent Communication
- Foundation for Enforcement
- Provide Evidence
- Limit Liability

Quality IT Policy DNA: MUSTS

- Business Strategy & Practices
- Implementable & Enforceable
- Concise & Easy to Understand
- Balance of Protection with Productivity
- Trust Model

Trust Models

- Trust Everyone All the Time
- Trust No One at No Time
- Trust Some People Some of the Time

Quality Policy DNA: Shoulds

- State Why Required
- Describe What is Covered
- ID Owners & Contacts
- Define Responsibilities
- How Enforced

Policies in Real Life

- Good People Comply!
- Bad People Break!

Are Good Policies Enough?

- Policies Provide a Foundation
- Procedures & Controls
- Education & Training
- Technology & Tools
- Management Leadership & Support
- Monitoring & Enforcement

Why Policies Fail

- Barrier to Progress
- Lack of Awareness
- Culture-Expect the Unexpected
- Non-Continuous
- It's too Complicated
- No Accountability
- No Enforcement

Implementation

- Risk Assessment
- Strategy & Policies
- Process & Controls
- Testing
- Monitoring & Updating

Good IT Policy Design

- Team Approach
- ID Governing Group
- Decide on Scope & Goals
- Decide on the Form & Substance that Works for You!
- Test the Policy-Does It Work?!
- Awareness & Education

Who do Policies Affect?

- Employees/Members-How You do Things!
- System Support-Implement, Comply, & Support
- Managers-Protection of Data, Cost
- Execs, SC, & Board- Reputation & Member Responsibility, Compliance

Key Policies-Must Have's!

- Acceptable Use
- Remote Access
- Information Protection
- Perimeter Security
- Host/Device Security
- Risk Assessment
- Password
- Virus Protection & Prevention
- Incident Response
- Business Continuity & Disaster Recovery
- 3rd Party Service Provider
- Wireless Communication

Procedures & Controls = The How

- Detailed Actions
- Quick Reference
- Eliminates a Single Point of Failure

Designing Security Controls

- IT Access Controls
- Physical Access Controls
- Encryption of CMI
- Member Information System Modifications
- Dual Control, Segregation of Duties, Background Checks
- Monitoring Systems & Procedures to detect attacks, intrusions, or extrusions
- Incident Response
- Destruction, Loss, or Damage of CMI



Reg 748 Part A Compliance

- Active Security Program
- Board Involvement
- Risk Assessment Process
- Manage & Control Risk
- Oversee Service Providers
- Monitor & Adjust
- Reporting

Why A Security Program?

- Ensure the security & confidentiality of member
- Protect Against Anticipated Threats or Hazards or Integrity of the Information
- Protect Against Unauthorized Access
- Ensure Proper Storage & Disposal of Member Information

Risk Assessment Guidelines

- Identify Reasonably Foreseeable Internal & External Threats
- Assess the Likelihood & Potential Damage of Identified Threats
- Assess the Sufficiency of Policies & Procedures

Develop & Implement a Response Program-Reg 748 B

- Assess Nature & Scope of the Incident
- Prompt Notification to Feds/State
- Notification to Law Enforcement
- Measures to Contain & Control Incident
- Notify Members when Warranted

Success!

- Board= Commitment
- Management=Leadership, Culture, Enforcement
- Employees= Compliance & Productive
- Members = Satisfied & Confident
- Regulators = Compliant

Resource Guide

- CERT
- FFEIC
- ISAC
- NCUA
- SANS
- Pivot Group

Today's Take Aways

- IT Policies Are Critical
- DNA of Effective Policies
- Provide Knowledge & Direction
- Be Involved & Committed
- Continuous Improvement
- Challenge = Competitive Advantage



Questions?

Thank You

Jim Soenksen

CEO

Pivot Group

404-419-2163

jsoenksen@pivotgroup.net