Driven to ISO- 27001 …

Driven by ISO- 27001 …

PRESENTED BY
JOHN VERRY
PRINCIPAL SECURITY CONSULTANT
PIVOT POINT SECURITY

Specialists in Security Assessments, Penetration Testing,
ISO 27001 & Security Information Event Management

ISO 27001 Will Be The Most Important Information Security Standard Of This Era

1) Why
   I. Flatter World
   II. Growth of ambiguous regulations
   III. The "Cloud"

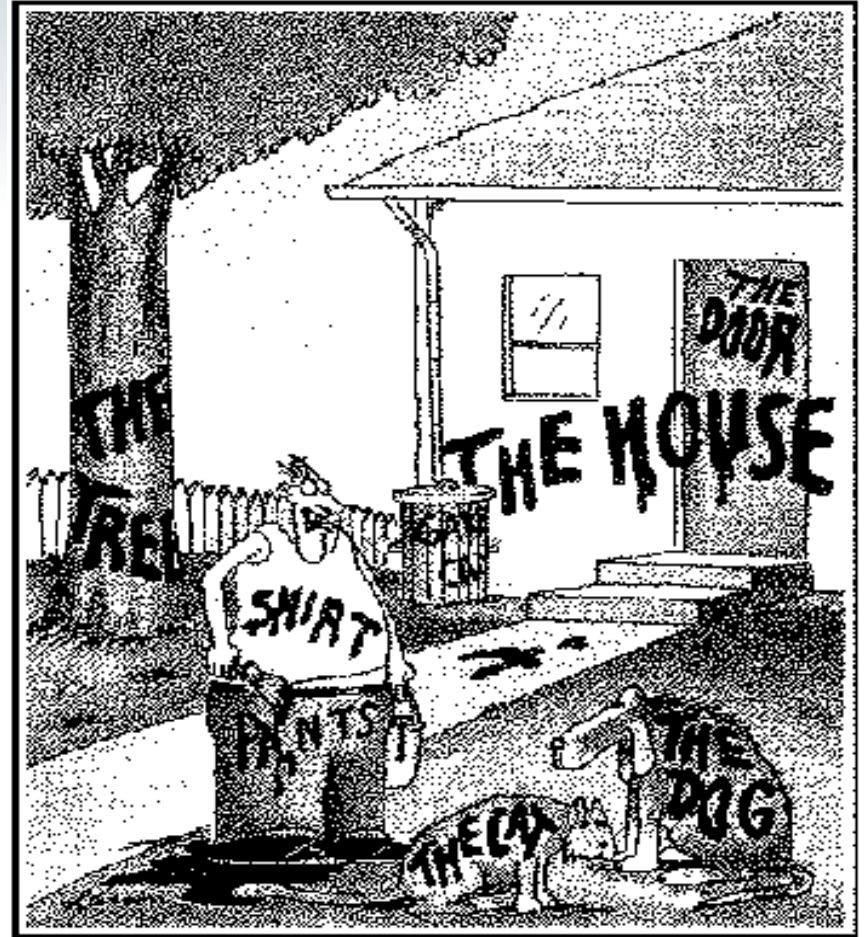2) How 27001 simplifies dealing with these issues

3) What we have learned from our 27001 customers

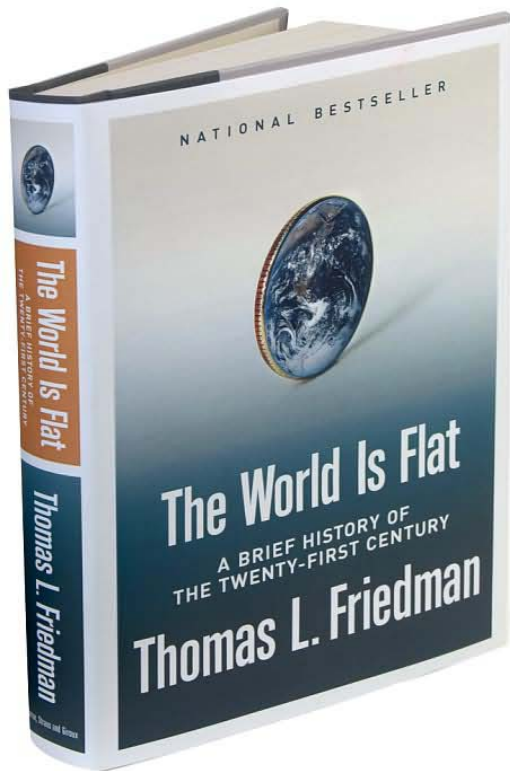4) Implications of the prediction being right

Quick Background

- 20+ years broad IT experience

- Info Sec Auditor exclusively for the last 9 years (CISA, 27001 Lead Auditor)

- PPS pure-play security assessment firm (audits/pen tests/SIEM)

- Diverse client base

"Now! ... That should clear up a few things around here!"

Driver #1: A Flatter World

Forces that have flattened the world:

Globalization

Out-sourcing & Off-shoring

The net, search engines, e-Commerce

The same forces impact information security (and are inputs to the next two drivers):

Collapsed/common security requirements

Third -Party Attestation

Mastering business is mastering technology

Driver 2: Ambiguous Regulations

47 + PII Regulations

FTC, PCI, NERC, HIPAA, HITECH, PCI-DSS, SARBOX, NIST/FISMA, etc.

"Control of User ID's"

"Reasonable monitoring"

Ambiguity Example:
Secure PII for 400K Employees

Engaged legal to ensure security requirements were complete

- More Guidance = More Ambiguity
  - Ambiguity in standard
  - Ambiguity in applying the standard
- The target changed before the remediation was complete
- Business requirements evolved creating PII where there was none
- Data/systems subject to other regulations (e.g., HIPAA, internal)

Driver 3: More w/ Less Drives Cloud

Economic & Business Drivers

- ✓ Fast, Good, Secure, Cheap (Pick 3)
- ✓ Driving Cloud Adoption

The Cloud Lures Uncle Sam

By MARK VEVERKA | MORE ARTICLES BY AUTHOR

Obama aims for the clouds.

Driver 3: Cloud Drives New Technology & Business Risk

Technology

- ✓ Automated Attack Tools
- ✓ SOA/Mashups

Hacking Takes Lead As Top Cause of Data Breaches

Hacking has topped human error as the top cause of reported data breaches since such tracking began in 2007, according to the Identity Theft Resource Center's 2009 Breach Report.

Facebook App Maker "RockYou" Sued Over Alleged Data-Breach

MONDAY, 04 JANUARY 2010 13:21 | FARUKH SHAIKH

Cloud Use Drives New Technology & Business Risk

Threat Agents

- ✓ Cyber-Espionage and State Sponsored Cyber-Terrorism

News > Technology > Google

Google attacks traced back to China, says US internet security firm

Why is 27001 the Answer to these changes?