



Ohio Information Security Conference '08

Bridging InfoSec and Business Objectives

Virgil Vaduva, CISSP, CISM
WinWholesale Inc.

- Guitar Hero
- Information and Knowledge
- Governance
- Strategic alignment
- Frameworks
- Examples & Research
- Q & A

Guitar Hero style security



O-ISC '08
Ohio Information Security Conference





A Heart Device Is Found Vulnerable to Hacker Attacks

By BARNABY FEDER
Published: March 12, 2008

To the long list of objects vulnerable to attack by computer hackers, add the human heart.

The threat seems largely theoretical. But a team of computer security researchers plans to report Wednesday that it had been able to gain wireless access to a combination heart defibrillator and pacemaker.

They were able to reprogram it to shut down and to deliver jolts of electricity that would potentially be fatal — if the device had been in a person. In this case, the researcher were hacking into a device in a laboratory.

The researchers said they had also been able to glean personal patient data by eavesdropping on signals from the tiny wireless radio that [Medtronic](#), the device's maker, had embedded in the implant as a way to let doctors monitor and adjust it without surgery.

SIGN IN TO E-MAIL
OR SAVE THIS

 PRINT

 REPRINTS

 SHARE

“Knowledge is fast becoming the sole factor of productivity, sidelining both capital and labor.”

Peter Drucker, *Management Challenges for the 21st Century*

Question

As a security professional, how can I enable my organization to make or sell more widgets for more dollars in order to increase the value for shareholders?

- Value Information and Knowledge
 - Confidentiality, integrity, availability
- Practice Governance
- Strategic approach
- Adopt frameworks
- Compliance strategy
- Cultivate research



“Indeed, without one security architecture, evidence suggests that enterprises will default to a haphazard, reactive, tactical approach to constructing a secure environment, regrettably wasting resources and introducing more vulnerabilities as they proceed to fix others.”

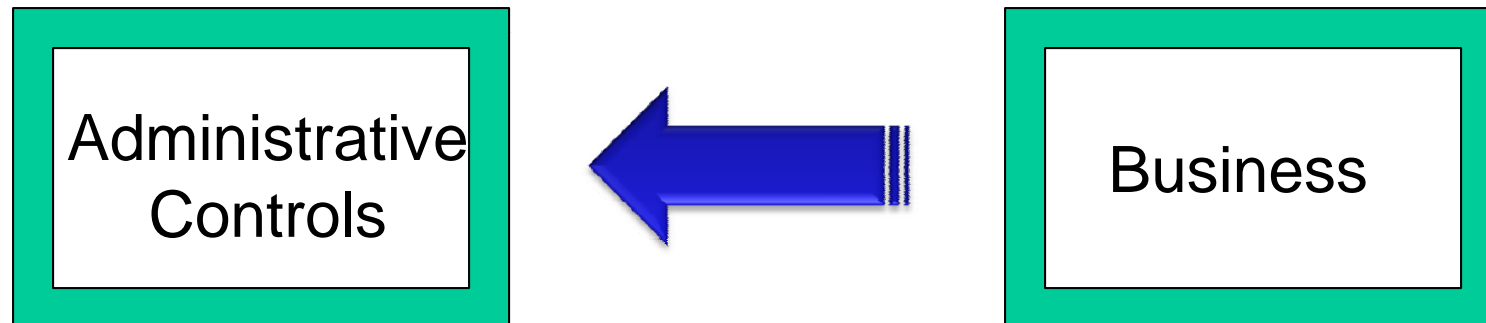
- *The META Group*

- Security not seen as enabler
- Lack of policies & governance
- No operating frameworks
- No alignment with business
- No concern for information; security is technology

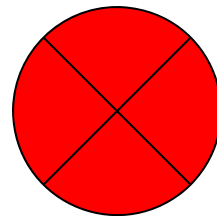
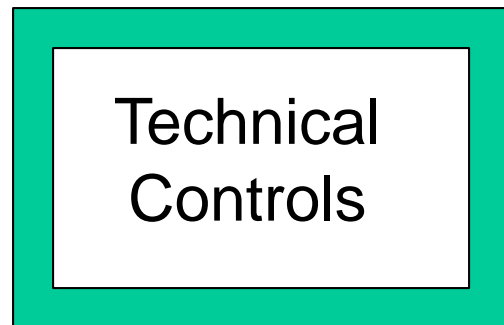
“The diffusion of technology and the commoditization of information transforms the role of information into a resource equal in importance to the traditionally important resourced of land, labor and capital”

Peter Drucker, *Management Challenges for the 21st Century*

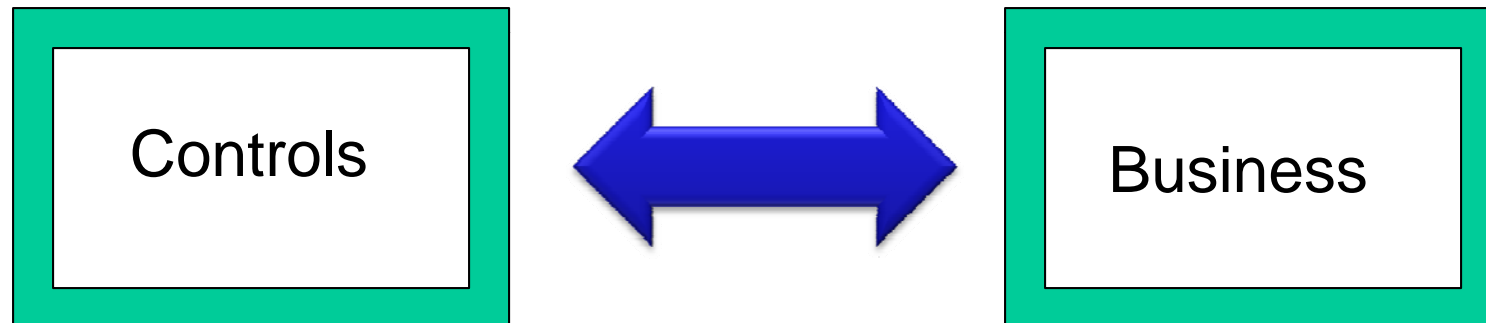
Problems



Problems



Solution

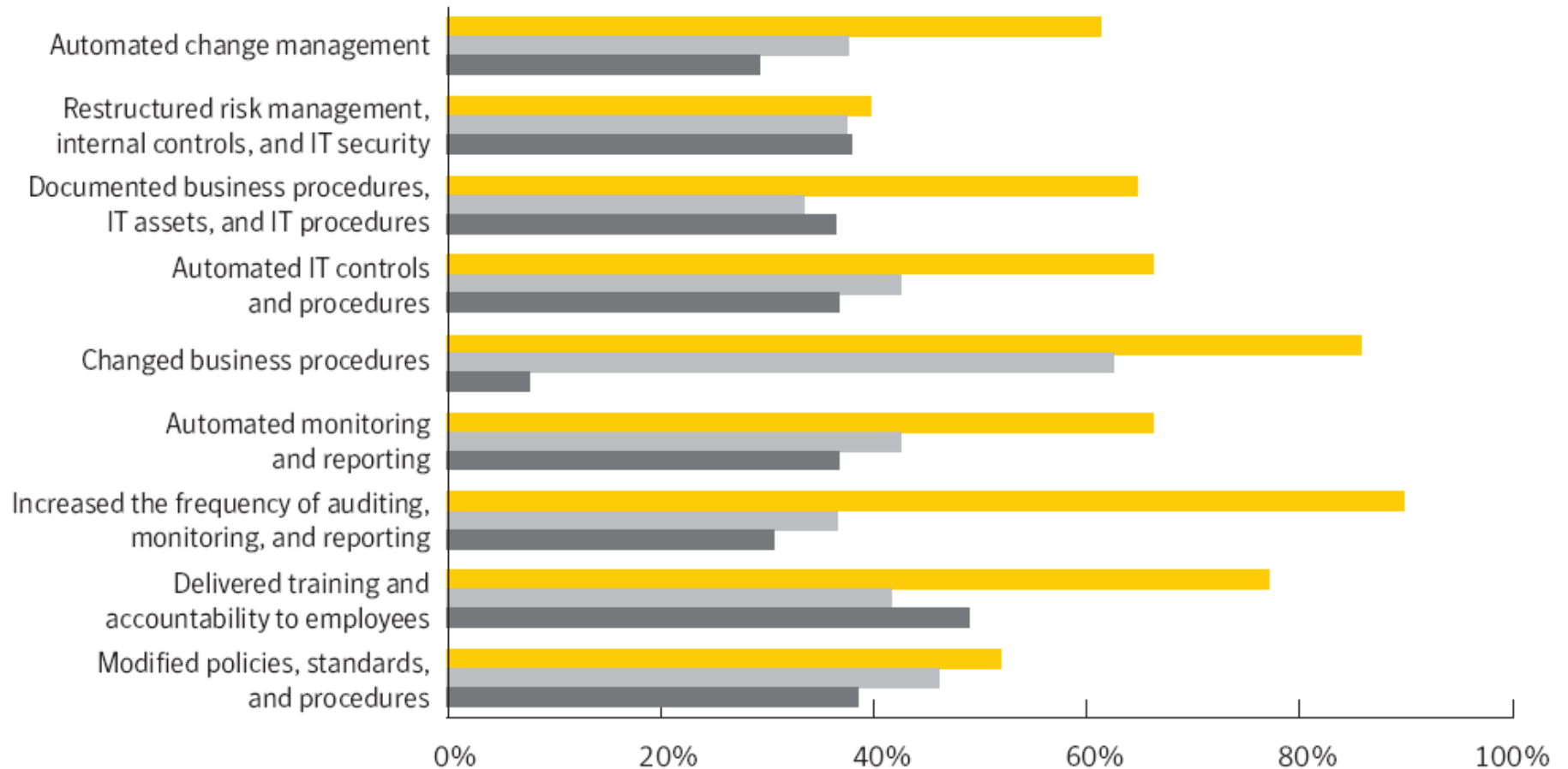


Symantec's Story



- Continuous training
- Restructure risk management
- Reallocate IT expenditures
 - Shift consultant spending to automation tools
- Automate measure tools, reporting, change management, policies
- Focus on managing risk

Symantec's Story

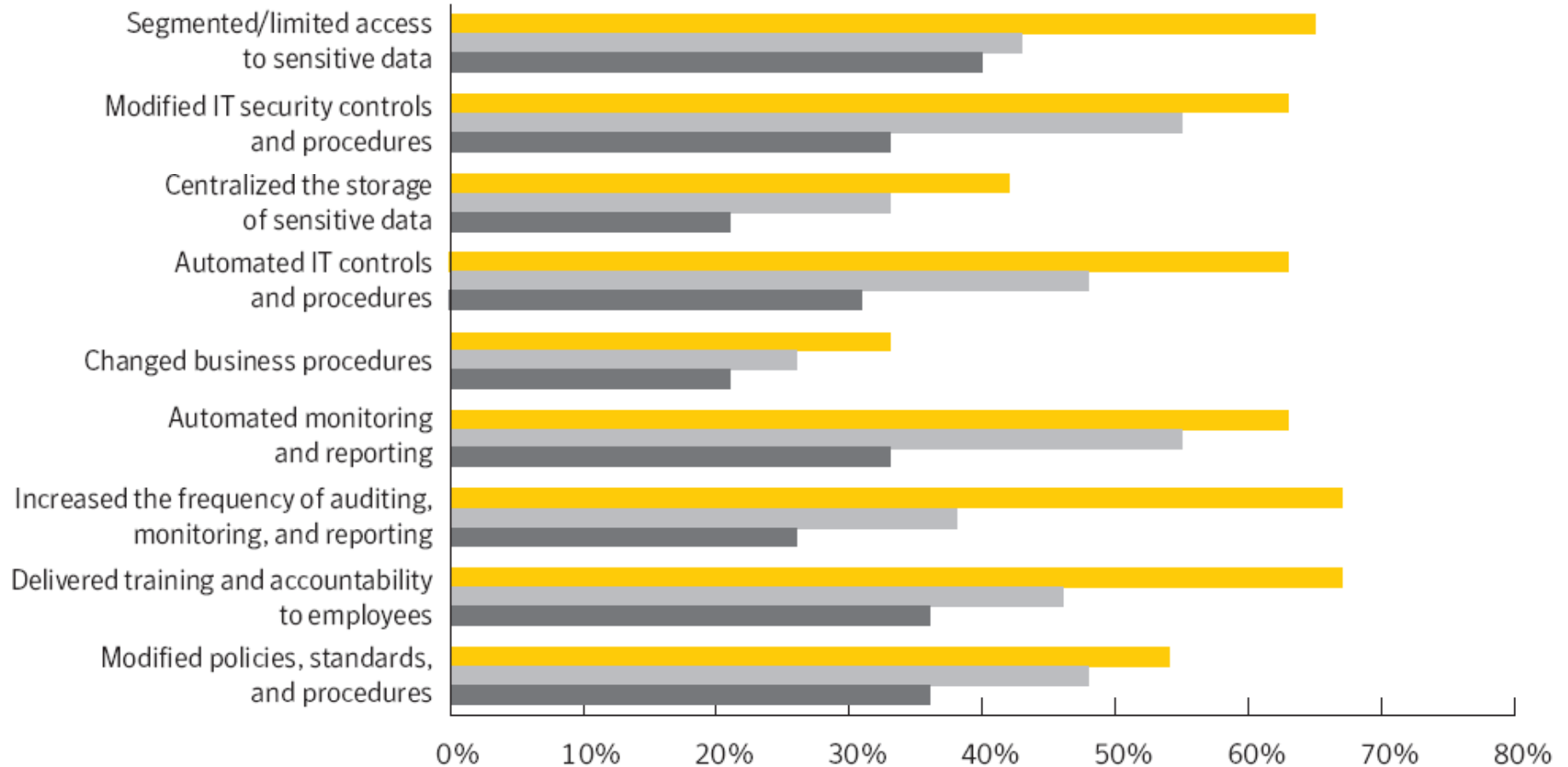


N: 1,330

Percentage of organizations

- Fewest IT control deficiencies
- Normative IT control deficiencies
- Most IT control deficiencies

Symantec's Story



N: 201

Percentage of organizations

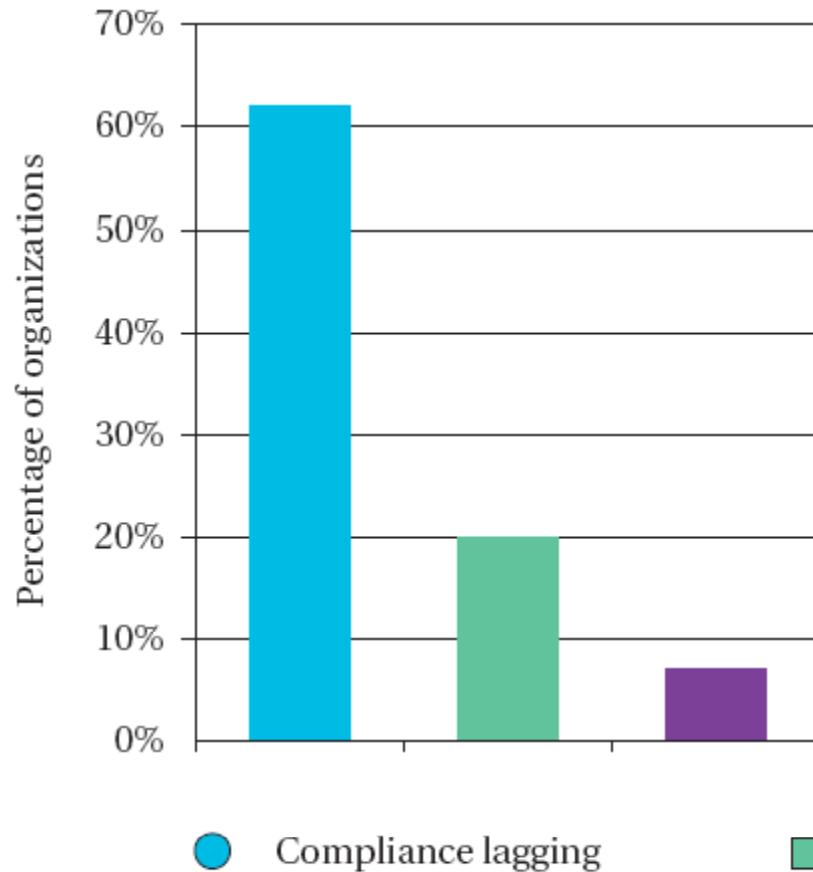
- Fewest losses of sensitive data
- Normative losses of sensitive data
- Most losses of sensitive data



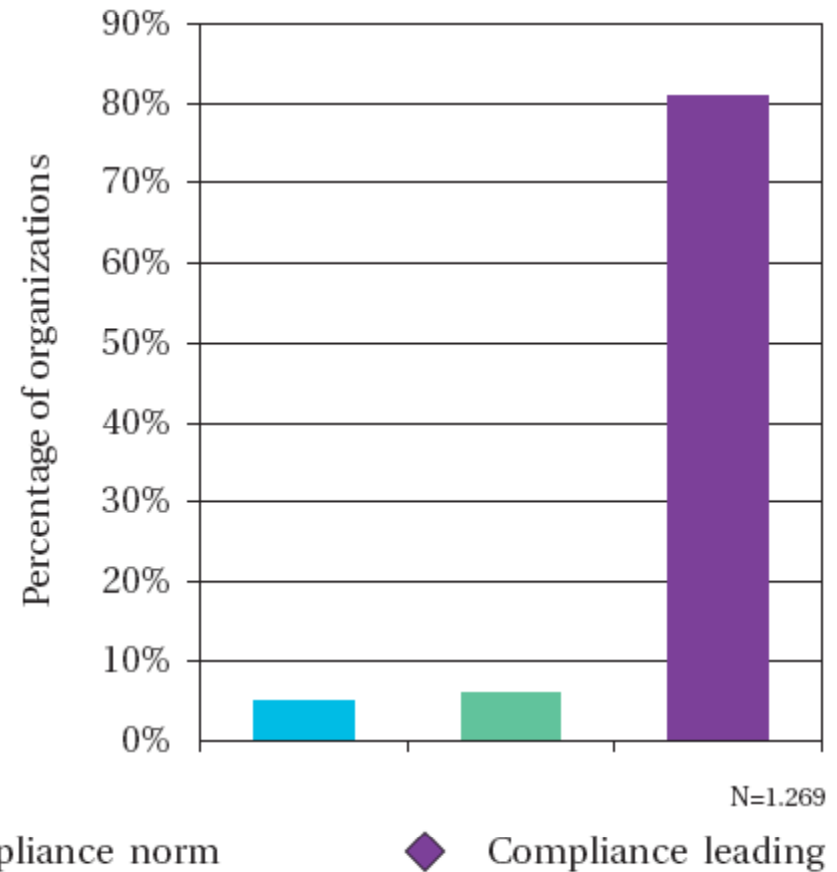
- 17 or more IT disruptions/year
- 22 or more data losses/year
- Financial loss every 3 years
- 8 percent temporary revenue decline
- \$100 cost per lost customer record

Cost of compliance

Seventeen or more annual business disruptions from IT security events

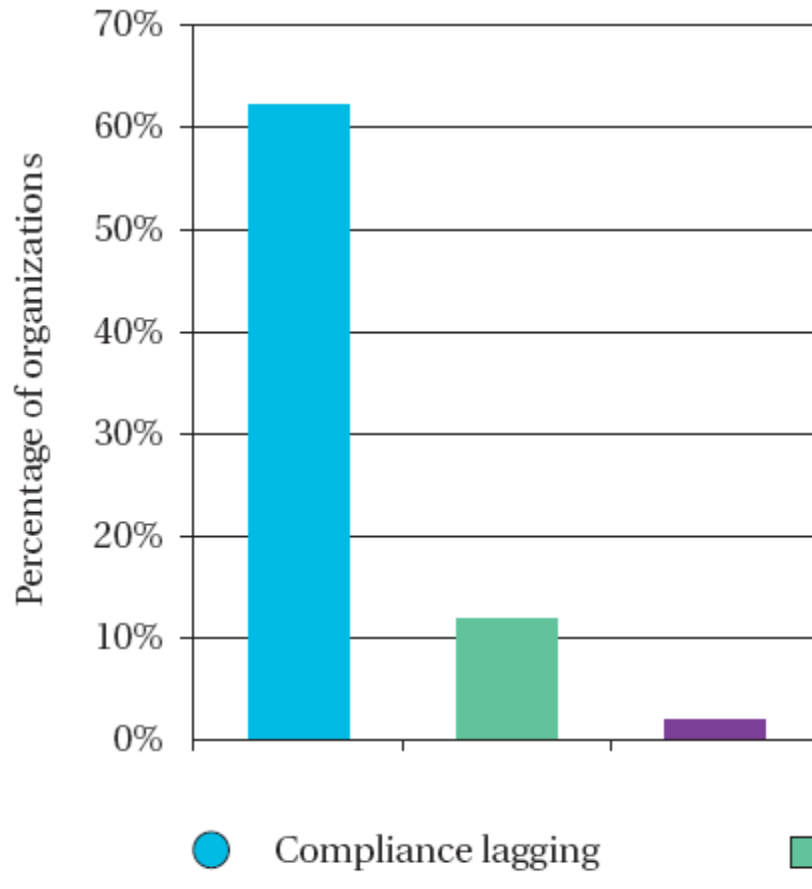


Two or fewer annual business disruptions from IT security events

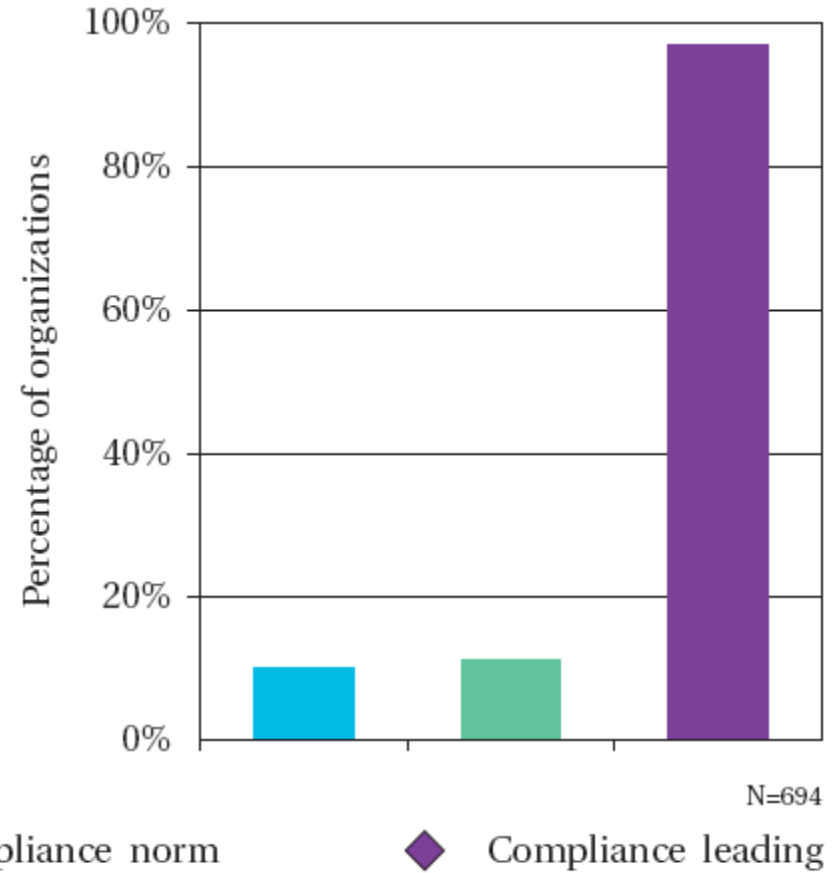


Cost of compliance

Twenty-two or more annual losses or thefts of sensitive data



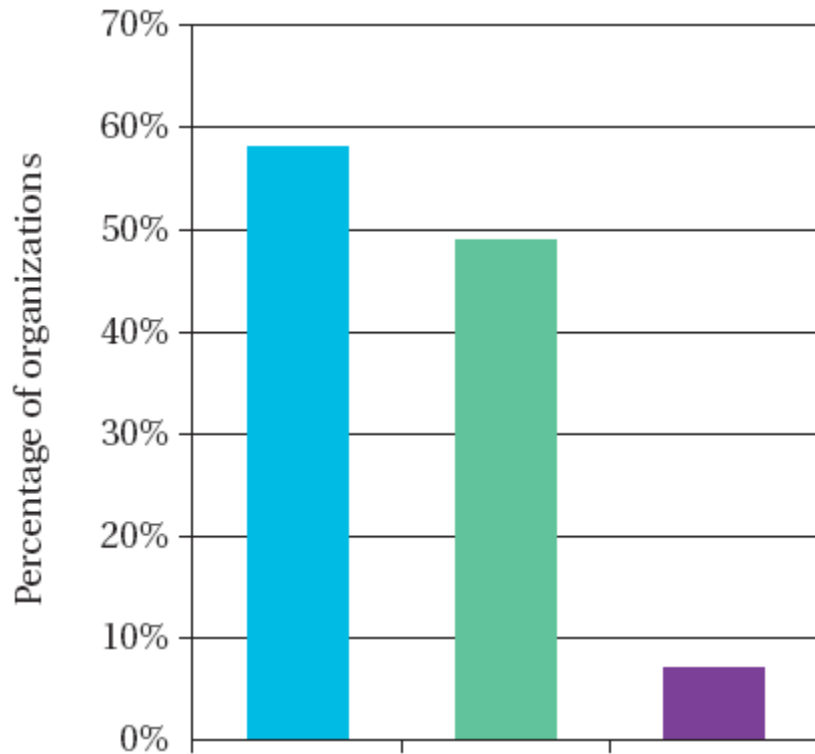
Two or fewer annual business losses or thefts of sensitive data



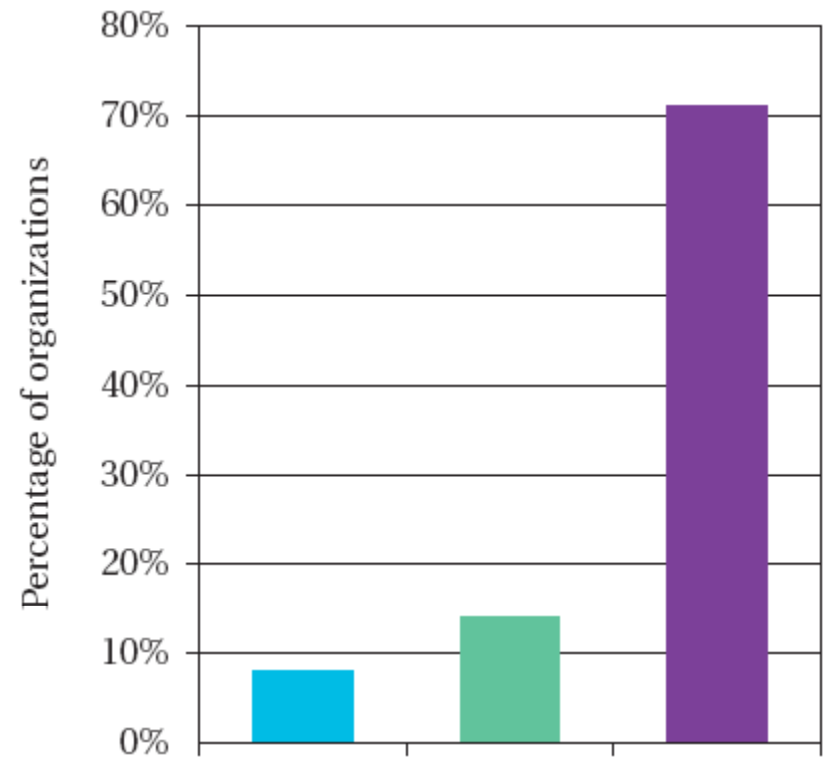
N=694

Cost of compliance

Three or less different IT security controls



Fourteen or more different IT security controls

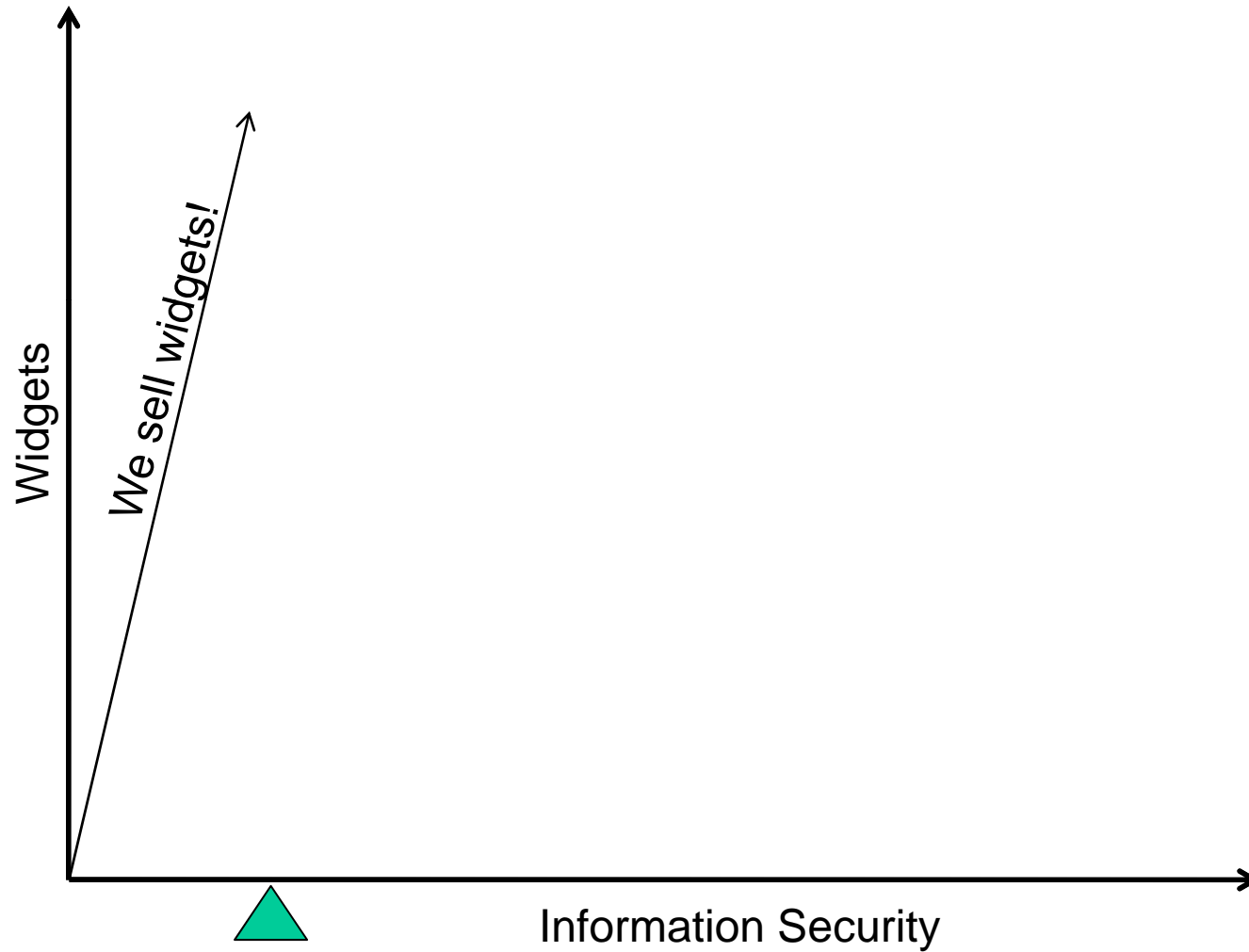


N=694

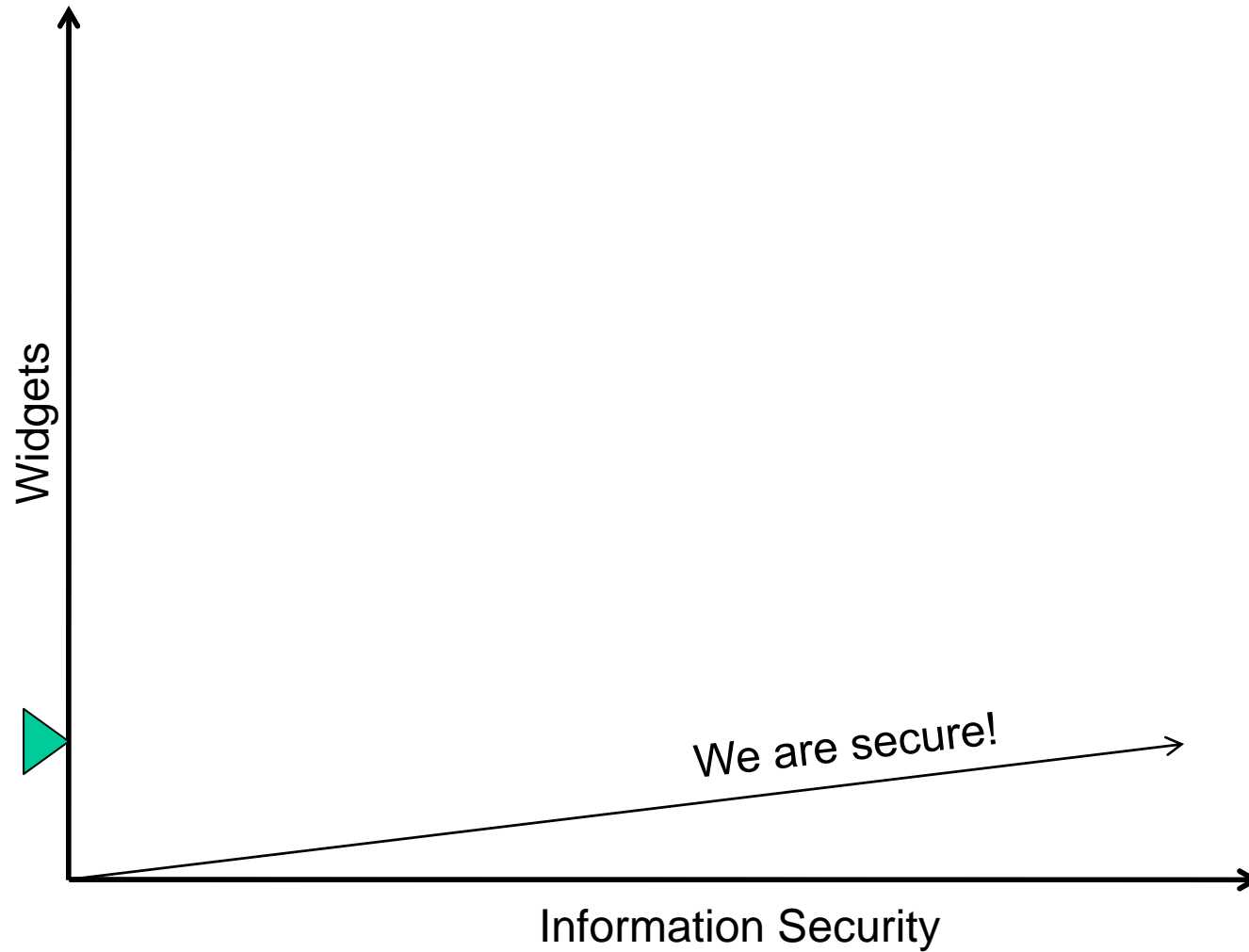
● Compliance lagging ■ Compliance norm ◆ Compliance leading

2007 IT Policy Compliance Group

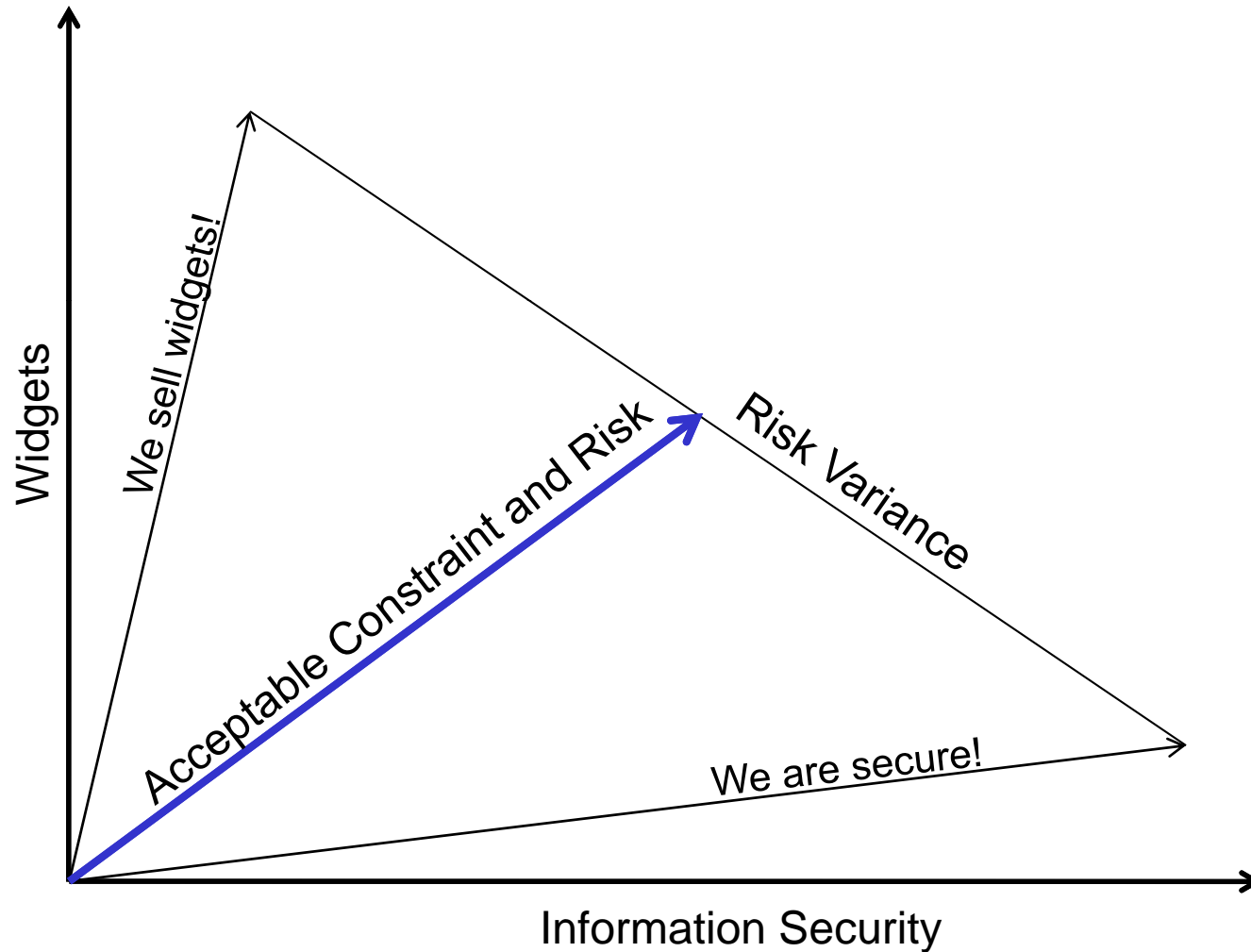
Unbalanced constraint



Unbalanced constraint

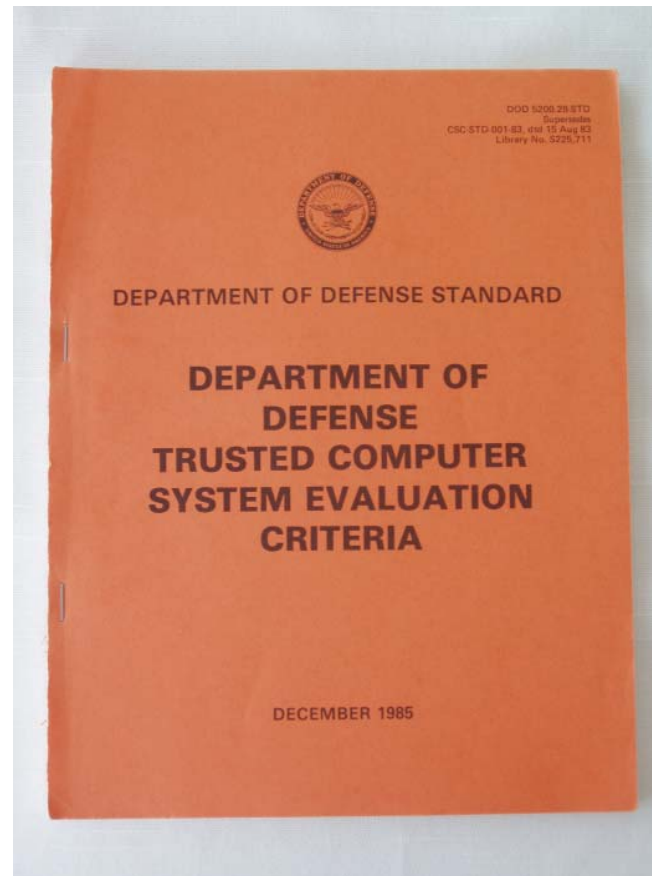


Acceptable constraint



- Policy development
- Policy enforcement
- Frameworks
 - ISO 15408 (common evaluation criteria)
 - COBIT (best practices framework)
 - COSO (internal controls framework)
 - ISO 27001 (security framework)

- Common criteria for Information Security Technology evaluation (or CC)



- Common criteria for Information Security Technology evaluation (or CC)
- TCSEC Orange Book
- DoD 5200.28M
- EALs, structure, purpose of evaluation
- Iso.org



- ISACA control objectives
- IT Management, users, auditors
- Version 4.1
 - Plan and Organize
 - Acquire and Implement
 - Deliver and Support
 - Monitor and Evaluate



- Criteria for assessment
- AICPA, AAA, IIA, FEI, MAI
- General management framework
 - Effective/efficient operations
 - Accurate financial reporting
 - Legal compliance

- InfoSec Management System (ISMS)
- ISO 27002/17799
- Process approach
- PDCA
 - Establish the ISMS
 - Implement the ISMS
 - Monitor the ISMS
 - Maintain and Improve the ISMS
- Compatible with ISO 9001 and ISO 14001
- ISO 9001 certification springboard

Common factors

- Comprehensive Strategy
- Governing policies
- Standards
- Organizational structure
- Process approach
- Metrics and feedback

- Board of directors
- Executive management
- Steering committee
- CISO
- Information Security Manager
- InfoSec Professional

“Firms operating at best-in-class security levels are lowering financial losses to less than 1% of revenue, whereas other organizations are experiencing loss rates that exceed 5%”



Questions & Answers