



University of Akron Symposium

February 2004

Information Security & Global Information Flows

D. Timothy Hartzell CISSP, CISM

Protiviti

www.protiviti.com

- ❖ About Protiviti
- ❖ Security/ Privacy Regulations in the U.S.
- ❖ State Laws
- ❖ Case Study 1
- ❖ Global Issues
- ❖ Case Study 2



About Protiviti

Robert Half International Inc.

- World's leading specialized staffing and consulting services firm, and the first and largest specialist in the placement of accounting, finance and technology professionals
 - Founded in 1948
 - More than 325 offices worldwide
- Member of the S&P 500
- Named one of “America’s Most Admired Companies” – and number one in the staffing industry – by Fortune magazine for fourth straight year
- Featured on Forbes Platinum 400 list of the best big companies in America
 - Fourth consecutive year
- 2003 revenues: \$2 billion

May 2002 – 650 people, 25 U.S. offices

While the Protiviti name is new, our people and their work remain the same.

Protiviti has obtained the exclusive right to the methodology, technology and knowledge resources that were developed by Andersen over the previous 13 years.

This combination of experienced professionals working with familiar tools allows us to offer world-class services to our clients from day one.

Now – Over 800 people, 29 offices in U.S. and 5 International

Who We Are

- We specialize in helping clients identify, measure and manage operational and technology-related risks within their industries and throughout their systems and processes

INDEPENDENT

We deliver unbiased, objective advice in the best interest of our clients – *No conflicts of interest*

RISK

We identify, source, measure, prioritize and help you manage the risks that stand between you and your goals

CONSULTING

We transform knowledge into real-world solutions that are functional and integrated into your organization

- We are an autonomous subsidiary of Robert Half International Inc.

"I want to congratulate you on your internal audit report - the sales commission review was really thorough. I've been working on various points of this issue - your report is really helpful to me. I would very much like you and your folks to do a follow-up audit in two quarters to help us drive some behavior changes. Thanks for your great efforts and results."

John Chen
President & CEO, Sybase

Internal Audit

Protiviti provides a full spectrum of management services for the continual transformation of internal audit functions, including:

- Full Outsourcing
- Co-sourcing
- Quality Assurance Reviews
- Internal Audit Transformation



"I have met with four of the Big Five firms to discuss our internal audit needs, and each firm has represented to me that they are participants in this service area. However it is clear to me that * Protiviti Consulting is the only firm that has the experience and the expertise to execute internal audit work effectively."

Jack Bell

Director - Audit Committee, Asyst Technologies

Business Risk Consulting

Protiviti provides a full spectrum of business risk management services. Our fields of specialization include:

- Credit
- Financial Commodities
- Treasury
- Revenue Management
- Contract Management
- Fraud
- Environmental / Assurance
- Legal and Regulatory



“Flexibility, highly skilled resources with a tremendous handle on best practices, better audits, comparable cost: * Protiviti Consulting was exactly what we had been looking for. Tektronix’s Audit Committee is very, very pleased with what’s transpired.”

Carl Neun
Senior Vice President and CFO, Tektronix

Technology Risk Consulting

Protiviti provides a full spectrum of technology risk management services. Our fields of specialization include:

- Security and Privacy
- IT Operations
- Business Systems Control and Effectiveness
- Business Continuity / Disaster Recovery
- Information Systems Testing
- IT Asset Management
- Project Management



All those in favor of a truly independent risk consulting and internal auditing firm ...

Say i



Information Security and Privacy in The U.S.

Increased Oversight and Compliance

<u>Governance</u>	<u>Date</u>	<u>Type</u>	<u>Industry</u>
1. HIPAA	8/1996	Security & Privacy	Healthcare
2. GLBA	5/1999	Security & Privacy	Financial Services
3. IIA—NACD	2/2000	Security Governance	Corporations
4. GISRA	6/2001	Security Standards	Government
5. FERC	7/2002	Security Standards	Energy
6. Sarbanes—Oxley	7/2002	Internal controls	Public companies
7. NYSE & NASDAQ	8/2002	Internal controls	Public companies
8. National Strategy	9/2002	Secure Cyberspace	5 Levels, Corp & Gov

Information Security Governance

IIA—NACD: What Directors Need to Know

1. **Accountability:** Who is responsible?
2. **Awareness:** How is it communicated?
3. **Ethics:** How to ensure ethical use of information?
4. **Inclusion:** Are all affected parties involved?
5. **Resource Allocation:** Are security investments commensurate with risk?
6. **Thoroughness:** Is security integrated throughout?
7. **Effectiveness:** How to avoid impact of IT failures?
8. **Ongoing Assessment:** How to ensure periodic audits or assessments?
9. **Compliance:** Are security measures fair and legal?
10. **Information Sharing:** How to share with peers and government?

Information Security Governance

Commonality

Secure your systems

Ensure good controls

Documented policies and procedures

Provide accountability

GLBA

- banks
- mortgage brokers
- mortgage lenders
- automobile dealers
- insurance companies
- real estate agents
- appraisers
- thrifts
- securities firms
- financial planners
- credit card companies
- credit unions
- data processors
- debt collectors
- retail stores that issue credit cards
- consumer reporting agencies
- mortgage brokers
- check-cashing businesses

State Law

State Law

California SB 1386

Became effective July 2003

All companies doing business in CA

Must notify any individuals whose PII was potentially compromised by a cyber attack.

State Law

California SB 1386

Personal Information

First name or initial with last name and

- ❖ SSN
- ❖ Drivers License Number or CA id card number
- ❖ Account number, credit or debit card number

State Law

Printing of more than the last four digits of a credit or debit card number prohibited in:

AR, AZ, CA, CO, IA, IL, LA,
KS, ME, MN, MO, NV, ND, OH,
OK, TX, VA, WA

Pending in:

KY, MI, NY, NC, PA, RI

Case Study 1

Why Security?

Why Security?

Victoria's Secret customers exposed

Glitch at web site allowed shoppers to take a peek..... at other customer's orders

The flaw made it possible to see what kind of knickers other people were buying

A shopper discovered the panty raid flaw

Why Security?

New York Attorney General sorted through Victoria Secret's dirty undies

Company agrees to \$50,000 fine to state of New York

Full refunds or credits to New York customers for having their g-strings paraded around the Internet

Global Issues

EU Data Protection Directive

Prohibits transfer of personal information to countries that do not ensure “adequate” protection

Adequate defined by the EU:

National regulatory law encompassing the entire private sector

National regulatory agency assigned to enforce it

EU Data Protection Directive

U.S. not in compliance

For companies doing EU business it may mean:

- Fines

- Disruption of service (TDF)

- Business operations suspended

- Bad press

- Harm to reputation

Recent Efforts

Canadian Standards Association

Protection of personal Information

International Privacy Standards

ISO

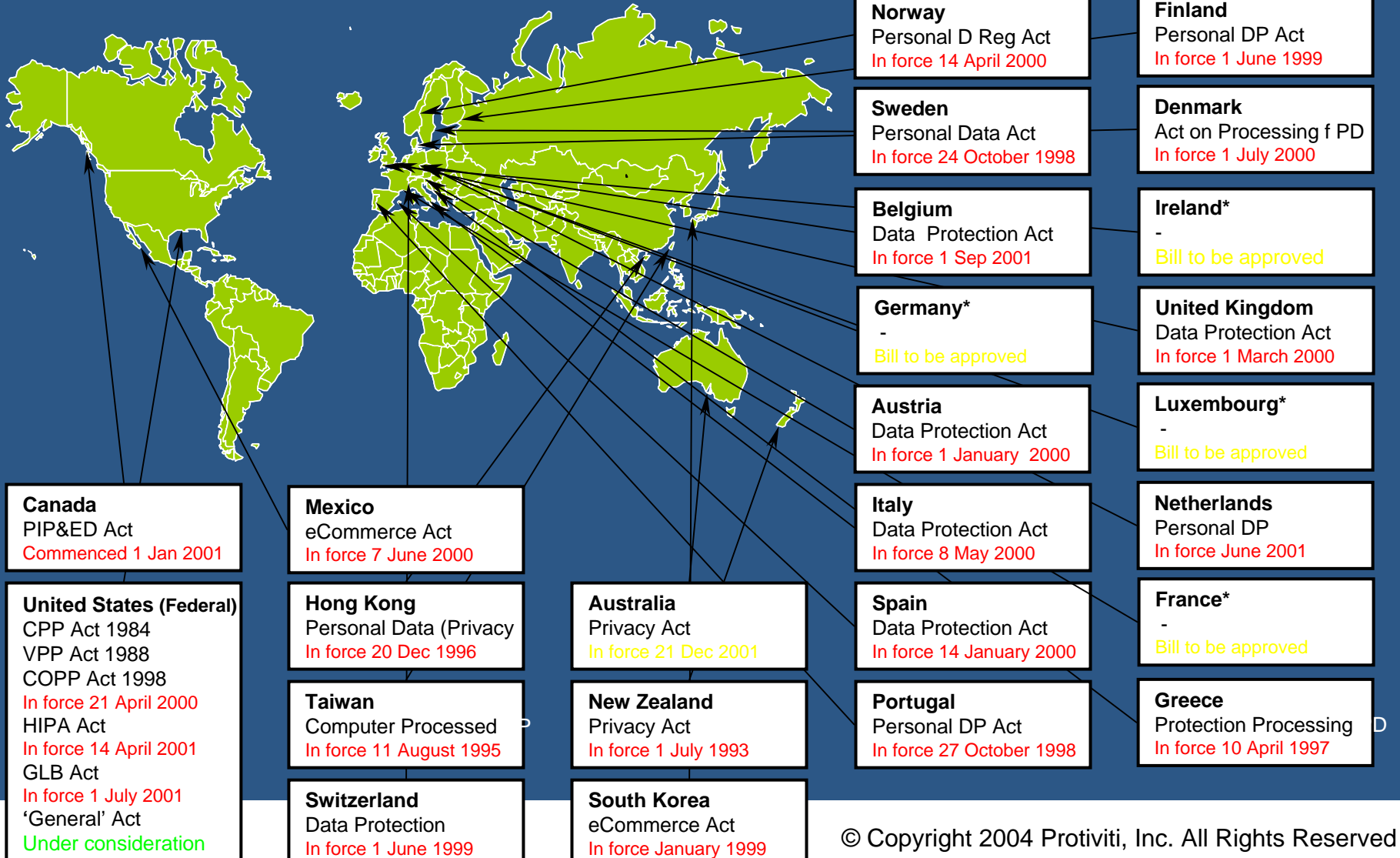
Multinational telecommunications alliance

National Private Sector Privacy Legislation Timeline (Industrialized Countries)

Business Risk

Technology Risk

Internal Audit



Case Study 2

Why Privacy?

Why Privacy?

- ❖ Philip Cummings
- ❖ Help Desk Employee
- ❖ 65 Person company
- ❖ Employed less than 1 year - Left March 2000



Cummings – faces over 30 years

Feds Crack Largest ID Theft Ring in U.S. History

- ❖ 30,000 victims
- ❖ Over \$2.7 million losses

Why Privacy?

- ❖ Sold credit report for \$30
- ❖ Ford Motor Credit Corp. found after reviewing bill
- ❖ Washington Mutual Bank
- ❖ Washington Mutual Finance Co.
- ❖ Dollar Bank
- ❖ Central Texas Energy Supply

Why Privacy?

**80% of all break-ins occur
from the inside!**

Change passwords!

Other Security Issues

Recent Worm Attacks

SQL Slammer

- Unknown installations of SQL server
- Laptops – home broadband no firewall
- Propagated on port 1434
- Companies hit through VPNs
- Only 376 bytes
- PATCHES AVAILABLE

Recent Worm Attacks

W32.Blaster

- Exploited DCOM RPC
- Laptops – home broadband no firewall
- Propagated on port 135
- Companies hit through VPNs
- PATCHES AVAILABLE

End User Awareness of IT Security

Security Awareness

Issues

- Lack of understanding
- Unaware of risks/consequences
- Policies not disseminated properly

Awareness training

- Must have formal program
- Use existing newsletters/ emails
- Must be continuous

Assessment

- Social engineering

Questions?

Protiviti, Inc.

625 Liberty Avenue

Suite 2501

Pittsburgh, PA 15222

D. Timothy Hartzell CISSP, CISM

Office: 412-402-1714

Mobile: 412-956-0838

Fax: 412-402-1797

timothy.hartzell@protiviti.com