# CERT'S PODCASTS: SECURITY FOR BUSINESS LEADERS: SHOW NOTES

## Information Compliance: A Growing Challenge for Business Leaders

**Key Message**: Directors and senior executives are personally accountable for protecting information entrusted to their care.

**Executive Summary**

The protection of information and information security are now legal, compliance, and liability issues. Information protection and due care with respect to security require that board directors and senior executives take action to comply with an ever-increasing number of laws in order to protect themselves, their shareholders, and their organization's reputation.

In this podcast, Thomas Smedinghoff, an attorney and partner in the Privacy, Data Security, and Information Law Practice at the firm of Wildman Harrold, discusses how business leaders can more effectively deal with the proliferation of information security and privacy laws, regulations, and standards and identifies some steps for starting an effective compliance program.

---

**PART 1: INFORMATION COMPLIANCE OVERLOAD**

**The Growing Challenge Â– Competing Trends**

Today's businesses are increasingly global, having to contend with multiple jurisdictions.

In contrast, information security laws and regulations are increasingly becoming local (country, state, city). These are often vague and can be in conflict with one another (state to state, country to country).

Compliance requirements come in a variety of forms: laws, regulations, common law obligations, contractual requirements, standards Â– even requirements from trading partners.

This all applies to both information security and privacy and can run the gamut to include:

- breach notification
- credit card processing
- the use of US Social Security numbers
- the use of RFID (radio frequency identification) tags
- laws governing spyware, records retention, and records destruction
- identity theft
- pretexting
- the handling of electronic transactions

And the list keeps growing!

**Global Conflicts**

For example, the European Union (EU) regulates the privacy and use of personal data much more thoroughly than in the U.S.

The U.S. Sarbanes Oxley Act requires companies to have an anonymous whistleblower capability for employees to report when they see something wrong. The EU Privacy Directive prohibits this.

### Consequences of Non-Compliance

Risks and consequences will vary by jurisdiction. Some countries have more active enforcement than others.

The U.S. Federal Trade Commission (FTC) is looking at designating failure to provide adequate security for personal data as an unfair business practice.

Based on recent high-profile data breaches (such as TJX), litigation and class action lawsuits are increasing. Courts are starting to recognize a common-law duty to provide adequate security.

---

## PART 2: WHO'S ACCOUNTABLE? BOARD DIRECTORS AND C-LEVEL EXECUTIVES

### What Roles Are Responsible for Protecting the Business?

Legal trends are shifting the responsibility for information security and privacy to the board of directors and C-level executives.

What has historically been viewed as solely an IT issue is now becoming a corporate governance issue.

Today and going forward, many senior executives and directors are starting to take a much more active interest, understanding that they will be held personally accountable if they fail to take appropriate action.

This is an obligation that involves everyone up and down the organization and in all lines of business.

The National Association of Corporate Directors has addressed these responsibilities in a number of publications, to help raise awareness and get this topic on the radar screen for board directors.

Information security is now a legal, compliance, and liability issue. It requires legal attention. Legal counsel plays a key role in helping senior leaders ensure that they are meeting their legal obligation.

### What Level of Attention Do Information Security and Privacy Issues Require?

Given that business leaders are primarily concerned with running their organizations, how should they determine how much attention to pay to these issues? What is their priority in the overall scheme of things?

As you might expect, this varies. For organizations that are highly regulated or depend heavily on sound information flow and protection, information security and privacy issues and risks rank very high.

That said, we're getting to the point where all businesses are (or are becoming) totally dependent on IT and network communication systems. They can be vulnerable if these assets are not adequately protected.

Each leader needs to ask the question "How significant is information security and privacy to our livelihood?"

Stakeholders, investors, shareholders, employees, customer, and suppliers are increasingly impacted by a company's lack of security leading to a security breach. We are all connected and thus all equally vulnerable.

The effect on the bottom line is one of the key drivers here.

---

## PART 3: EFFECTIVE STEPS TO GET STARTED

### Putting a Compliance Program in Place

**First**, recognize that information security compliance is a continuous process involving risk assessment and evaluation, timely response to results, and periodic re-evaluation.

Identify what kind of data you have, its importance and sensitivity, where it is stored, who owns and is responsible for it, and who has access to it.

**Second**, review the data life cycle. How is data being created, acquired, and collected? How is data being used? Is it being destroyed when it is no longer needed and how? What are the relevant legal and litigation issues?

For example, with personal data, there are laws and regulations that dictate where you can acquire it from, where you can transfer it to, what you can do with it, and how you have to destroy it.

**Third**, clearly understand what laws apply to the data. You may need to consider multiple jurisdictions (local, state, national, international), focusing on those where you do the most business.

Understand the likelihood, penalties, and risk of non-compliance.

**Global Supply Chain Partners and the Virtual Enterprise**

Understand what data is yours (versus your partners). You are responsible for protecting your data regardless of where it resides or is being used.

When sharing or outsourcing data, consider:

- who you are working with and how trustworthy they are
- the procedures they have in place
- appropriate requirements to include in your contracts

Monitor ongoing data protection actions to ensure partners are doing what they say they will do.

**Resources**

Smedinghoff, Thomas J. "The State of Information Security Law." November 2007.

Smedinghoff, Thomas J. "Trends in the Law of Information Security." Presentation to the Security Management Conference, ISACA Winnipeg chapter, November 2007.

Smedinghoff, Thomas J. "Information Compliance Overload: Dealing with a Growing Corporate Legal Nightmare." Presentation to the Security Management Conference, ISACA Winnipeg chapter, November 2007.

Smedinghoff, Thomas J. "Director Responsibilities for Data Security: Key Questions the Board Should Ask." Directors Monthly, National Association of Corporate Directors (NACD), April 2007.

Smedinghoff, Thomas J. "Security Breach Notification Law: Defining a New Corporate Obligation." The Bureau of National Affairs, 2006.

Smedinghoff, Thomas J. "Where We're Headed-New Developments and Trends in the Law of Information Security." Wildman Harrold, Nov. 2006.

National Association of Corporate Directors. Â“Information Security Oversight: Essential Board Practices.Â” NACD, December 2001. Ordering information is available at http://www.nacdonline.org/publications

CERT's Governing for Enterprise Security portal