


A background image showing a laptop on a desk with a speedometer overlay. The speedometer has numbers from 0 to 60 and a needle pointing towards 40. The text 'Regulatory Compliance' is overlaid on the right side of the image.

## Regulatory Compliance

Trend Micro, Incorporated 

 **Protecting Sensitive Information in an Increasingly Leaky World**

A Trend Micro White Paper | March 2009

# Regulatory Compliance: Protecting Sensitive Information in an Increasingly Leaky World

## ➔ TABLE OF CONTENTS

I. REGULATION CREATES WAVES WORLDWIDE .....	3
II. COMMON THEMES RECUR .....	4
III. IDENTIFYING A FLEXIBLE COMPLIANCE STRATEGY .....	8
IV. SOLUTIONS FOR HELPING ACHIEVE COMPLIANCE – AND MORE .....	10
V. SUMMARY .....	10
VI. EXHIBIT A .....	11

# Regulatory Compliance: Protecting Sensitive Information in an Increasingly Leaky World

Information technology (IT) security is indispensable to an organization's ability to conduct business and achieve its objectives. Security requirements affect almost every business process and system, and successful security measures help protect a business' brand value, stakeholder confidence, risk management strategies, and compliance status. Requirements vary among industries, geographies, and regions, but the need to protect privacy, retain important data, and facilitate e-discovery are common to all. This paper provides an overview of the regulatory landscape and identifies steps to take for defining a flexible compliance strategy.

## I. REGULATION CREATES WAVES WORLDWIDE

At its simplest, "compliance" is the adherence to an accepted policy or set of requirements. Policies can range from those that help the business avoid worst-case scenarios – such as customer churn, litigation, and fines for noncompliance – to the "should haves," including IT security standards and corporate mandates to protect its brand and stakeholder confidence.

Achieving – and maintaining – compliance requires more than just the hardware or software products that can provide automation. Enterprises must address compliance through employee training and enforcement. In global enterprises, achieving and maintaining compliance becomes even more challenging because they must comply with domestic and international regulations.

Although many nations and jurisdictions have had privacy laws on the books for decades, most were written for a paper-based world. Proliferating electronic data communication and storage have made data theft more damaging, and retrieving critical data has become considerably more challenging. For example, civil proceedings subpoena emails as evidence, often dating back several years, such as in cases of patent infringement or financial fraud. The vast volume of regulated electronic content has resulted in updated regulations to cover electronic communications.

In the U.S. alone, more than 700 state and federal privacy and surveillance laws existed in 2008 (Compilation of State and Federal Privacy Laws, Privacy Journal, 2008). In October 2008, the state of Nevada enacted a law requiring all businesses to encrypt all personally identifiable information (PII) – including names and credit card numbers – that are transmitted electronically. Other state laws, such as Massachusetts Standards for the Protection of Personal Information of Residents of the Commonwealth, apply to all organizations that maintain personal information about a Massachusetts resident – whether they do business in the state or not. This regulation outlines specific technical controls that are required, including encryption of all records transmitted across public networks and data encryption on all laptops or portable devices.

Although some regulations are voluntarily adopted, others are the result of industry or regional mandates, such as the European Union Data Protection Directive. This directive requires that member countries adopt standards for the collection, storage, and disclosure of personal data. An example of this ripple effect is the adoption of the Data Protection Act 1998 in the United Kingdom, codifying data protection requirements into local law.

# Regulatory Compliance: Protecting Sensitive Information in an Increasingly Leaky World

## II. COMMON THEMES RECUR

Although the number and complexities of laws in different jurisdictions can be overwhelming, common themes exist. Three common themes include privacy, data retention, and e-discovery. The following table summarizes a sampling of global regulations and their common requirements across these data protection areas.

Protected Data Types and Requirements	Description
PII: Personally Identifiable Information	Social security number/national identification number, drivers license number, address, phone number
PCI: Payment Card Industry	Credit card numbers, Card Verification Value (CVV), expiration date
PHI: Protected Health Information	Medical diagnosis codes, disease names, medication names, patient names
PFI: Personal Financial Information	Financial account number, credit score
PFI Access Control	Monitor privileged user access to company financial data, separation of duties for data and processes impacting financial reporting
Audit	Covers best practices to validate controls to address regulation

# Regulatory Compliance: Protecting Sensitive Information in an Increasingly Leaky World

## Common Themes Across Global Regulations

Figure 1: Common regulatory themes around the world

Geography	Regulations with Similar Data Protection Requirements				
	Privacy Regulations				e-Discovery, Data Retention
	PHI	PCI	PII	PFI, Access Control	
Global					
North America					
US	✓		✓	✓	✓
Canada	✓		✓	✓	✓
Europe					
EU	✓		✓	✓	✓
UK	✓		✓	✓	✓
Switzerland	✓		✓	Covers best practices for validating controls	✓
Germany	✓		✓	—	✓
Asia Pacific					
Japan	✓		✓	✓	
Singapore	—	✓	—	Covers best practices for validating controls	✓
Australia	✓		✓	Covers best practices for validating controls	✓
India	✓		✓	Covers best practices for validating controls	✓
Latin America					
Brazil	Proposed		Proposed	Covers best practices for validating controls	Proposed
Mexico	✓		✓	Covers best practices for validating controls	✓

# Regulatory Compliance: Protecting Sensitive Information in an Increasingly Leaky World

## Privacy

All of these regulations aim to protect individuals' privacy, usually by requiring that data associated with that individual is not visible to unauthorized users. Protecting individuals' personal, medical, and financial data is of utmost concern to enterprises for regulatory compliance, but also for fear of brand damage and ultimately, profitability. Just as customer and employee data is essential to a business, resident data is essential to a jurisdiction, and citizens expect their governments to safeguard their data.

Data confidentiality must also include intellectual property and other company-sensitive data to protect stakeholder interests and brand reputation. Some regulations, such as the UK Data Protection Act, go even further to mandate that an individual be notified upon data collection, such as when completing a web-based form, as to how their information will be used.

Although the specific data regulated varies among statutes, generally the key to enforcing privacy requires an ability to detect sensitive content, and report, block, or encrypt it. For example, protecting email and attachments from unwanted eavesdropping, tampering, and spoofing requires encryption, recently mandated by the state of Nevada to protect PII associated with Nevada residents. Approaches used to secure individual privacy can also be extended to secure other types of data. For example, content monitoring, content filtering, and Data Leak Prevention (DLP) solutions can be used for helping meet a wide range of compliance requirements.

## e-Discovery Requirements

Electronic discovery has become critical in a wide range of applications, such as for litigation support, when evidence must be produced in a court of law to prove or refute a claim. Requirements include the ability to search for specific data – including data stored over long periods of time – in a timely manner and produce results that maintain chain of custody to prevent tampering with evidence.

The emphasis on timeliness and correct format should not be overlooked:

- U.S. lawsuits have enforced Rule 16 of the Federal Rules of Civil Procedure, which requires that data be produced to the court within a short period of time from the request.
- Rule 34 of the same act requires data to be produced in its native format, such as an email with attachment.
- In Canada, Ontario Rules for Civil Procedure specify the timeframe to be “as soon as practicable.”
- Principle 11 of the same statute states that the data format can be agreed upon by the parties.

In most e-discovery laws, evidence accuracy is questioned if any suggestion is made of data tampering, data destruction, or non-disclosure of privileged user access. Questions usually damage the chain of custody and can render the evidence inadmissible.

# Regulatory Compliance: Protecting Sensitive Information in an Increasingly Leaky World

## Data Retention Requirements

Data retention requirements are mandated in support of right-to-information acts or in securities trades, which may be investigated years after the fact. Data retention laws vary across geographies but have the common theme of specifying that certain types of data be stored for specific periods of time. In Australia, the Corporations Act, Income Tax Assessment Act, and Archive Act mandate records retention for different time periods, albeit for different types of records. The European Union Directive 2006/24/EC requires Member States to ensure that communications providers must retain data for periods ranging from six months to two years.

## Privacy Pervades e-Discovery and Data Retention Requirements

Even though distinct regulations govern the three common themes of regulatory compliance – privacy, e-discovery, and data retention – privacy rules permeate e-discovery and data retention. Whenever data can be tied back to an individual or can be identified as business-sensitive – privacy is prioritized. In the case of e-discovery, producing evidence – such as email correspondence between an employee and a partner – requires that sensitive data is:

- Tamperproof with an audit trail (data integrity)
- Only viewable by authorized parties (access control)
- Protected from viewing by unauthorized parties (confidentiality through encryption)

Similarly, in cases of data retention, records must only be produced to entitled parties (access control), and if they contain sensitive data, they should be kept confidential.

The German Telecoms Data Retention Act interprets the EU directive and mandates that certain customer traffic data be retained for six months. However, the act has created complications arising from constitutional concerns about storing data on customers without cause. Until pending changes are better understood, employee and customer privacy remains the top priority, requiring that emails be archived in a secure manner to prevent theft and compromise. The privacy of stored records will continue to be scrutinized as retention laws are enforced and audited.

## Are Standardized Compliance Solutions Possible?

As some of the previous examples show, laws in different jurisdictions present common themes but contain enough differences to make it impossible to adopt a one-size-fits-all compliance solution. Organizations' compliance strategies must include solutions that support different policies for:

- Monitoring different data types
- Enforcing different data protection policies, such as report-only, block, or encrypt
- Searching, retention, and quality for archived data

# Regulatory Compliance: Protecting Sensitive Information in an Increasingly Leaky World

## III. IDENTIFYING A FLEXIBLE COMPLIANCE STRATEGY

Even with common privacy, data retention, and e-discovery elements, achieving compliance with all applicable regulations represents a significant undertaking, so creating a sound foundation is critical to achieving and maintaining compliance over time.

### **Determine Compliance Scope Using Risk-Based Approach**

Compliance is about passing the audit. IT auditors assess compliance by first establishing the scope of their audit. For example, they define which areas of the business are most likely to represent the data, stakeholders, and scenarios covered by the specific regulation.

In an ideal world, data protection would cover all networks and nodes where sensitive data is transported, stored, or used. This would include end-user systems, databases, file servers, email servers, and network gateways. However, this level of protection is unrealistic due to operational limitations. Instead, the focus of an audit should be on high-risk systems – infrastructure that is most commonly used or likely to present the greatest risk to the business, if compromised. One area to focus on is the group of insiders who are authorized to access sensitive data and systems under control of enterprise IT support. Employees and contractors with authorized access are being viewed as an increasing threat to the enterprise, as validated by a recent IDC survey of IT professionals (Oracle Database Security: Preventing Enterprise Data Leaks at the Source, February 2008, sponsored by Oracle Corporation and IDC). By focusing on high-risk areas, IT and audit resources can be efficiently allocated where they are most needed.

### **Begin with Email**

A good place to start is where data is most easily transmitted. In today's world, this would be email, including both corporate and public webmail systems. Some regulations clearly call out electronic communications as a risk area while others make general statements about protecting the specific data, leaving the business to determine the best method of protection.

Financial Industry Regulatory Authority (FINRA), the largest regulator of securities firms doing business in the U.S., published Regulatory Notice 07-59 "Supervision of Electronic Communications," which highlights the importance of detecting and monitoring email and other electronic communications for restricted, securities-related terms. "Electronic communications" covers the actual transmission of the data from the sender, to the mail gateway, and finally to the recipient. It also covers subsequent data storage on a mail or email archive server.

Risk inherent throughout data transmission and storage is high. For example, employees routinely download, create, paste, or attach sensitive data to their emails and send them to internal and external users. This is usually done without malicious intent and often with no awareness of their infraction, but these activities place the organization at considerable risk.

# Regulatory Compliance: Protecting Sensitive Information in an Increasingly Leaky World

Another common risk is data in use and kept on an end-user's device – desktop system, laptop, or mobile device. Without proper security, users can easily copy sensitive data to peripheral devices, such as USB storage, and can also email, instant message, and post data to websites. Stopping these risky behaviors at the source minimizes the risk of the data being transported to places unknown and is more effective than blocking at a network gateway, since the data may have already been intercepted on the network by an unauthorized user.

## **Implement Policy-based Solutions**

The tremendous variety of compliance regulations and their interpretations for various industries and jurisdictions makes it critical to adopt flexible protection solutions. Policy-based solutions provide the required protection with an ability to tailor security deployment and enforcement as needed. For example, one regulation may mandate encryption of PII data; others may require that sensitive data be monitored and protected, but do not specify how to do it. One organization may interpret that a “monitor and block” solution on end user systems is sufficient to address this requirement while another may decide to encrypt content at the user's desktop.

Still other regulations focus on data confidentiality and privileged access to this data. This would require policies that have end-user awareness through users' network identities or email addresses. Japan's Financial Instruments and Exchange Law (Japan FIEL) and U.S. Sarbanes-Oxley both require separation of duties and veracity in financial reporting, but Japan goes further to outline the IT security control environment, risk assessments, monitoring, and support. A policy-based data protection solution could address requirements for the Japanese branch of a multi-national company while also addressing less-prescriptive U.S. requirements.

## **Include People and Processes with Product**

Compliance cannot be solved with a product alone. It is a combination of people, products, and procedures that address regulatory requirements. People require training and education on sensitive data use policy. Procedures must be in place to secure the data lifecycle – creation, modification, storage, transmission and destruction. Products are deployed to automate as many of these processes as possible and to enforce controls. Integrating sustainable controls into existing infrastructure greatly increases likelihood of compliance.

# Regulatory Compliance: Protecting Sensitive Information in an Increasingly Leaky World

## IV. SOLUTIONS FOR HELPING ACHIEVE COMPLIANCE – AND MORE

Training employees and adapting processes to achieve compliance are essential elements of a compliance strategy. Success however, also depends on implementing proven, policy-based endpoint DLP, email encryption, and email archiving solutions.

### Endpoint Data Leak Protection

Data leak prevention solutions are designed to protect sensitive information, such as customer, employee, and patient data – as well as intellectual property – by monitoring and preventing information leaks across multiple threat vectors, including email, webmail, instant messaging, USB drives, and CD/DVDs. They identify sensitive data across laptops, desktops and servers, whether online or offline, using highly accurate content-matching and fingerprinting technology. Some solutions also help enforce organizational policy by preventing improper use of customer and employee information or educating employees about secure practices. Solutions such as Trend Micro™ LeakProof™ enable organizations to go beyond facilitating regulatory compliance by protecting privacy. They also help protect the organization's intellectual property by providing visibility and control over sensitive information on end user systems.

### Email Encryption

Email encryption solutions enable organizations to enforce compliance requirements and to ensure that confidential information is delivered securely. Policy-based encryption, available for Trend Micro InterScan™ Messaging Hosted Security, automates encryption for specific types of content to help achieve compliance.

### Email Archiving

Email message archiving solutions can automate storage and retrieval, accelerating access while securing messages to resist tampering. Trend Micro™ Message Archiver provides fast, easy search capability and reduced storage cost, while enabling e-discovery and compliance with data retention regulations.

## V. SUMMARY

The best approach to meeting complex compliance requirements is to focus on highest risk, most-used business systems and employ a combination of trained people, process enforcement, and policy-based security solutions. Trend Micro Data Protection solutions address privacy, e-discovery, and data retention requirements with email encryption, email archiving, and endpoint Data Leak Prevention solutions.

For more information, please visit [www.trendmicro.com](http://www.trendmicro.com).

# Regulatory Compliance: Protecting Sensitive Information in an Increasingly Leaky World

## VI. EXHIBIT A

### Regional Sampling of Regulations, Standards, Frameworks\*

#### Global

PCI DSS (Payment Card Industry Data Security Standard), ISO 19779/27001 (International Standards Organization) IT Security standard, ITIL (IT Infrastructure Library) framework for service delivery, COSO (Committee of Sponsoring Organizations) risk management in financial services, CoBIT (Control Objectives for Information and Related Technology) IT security standard

#### Americas

**US:** HIPAA (Health Insurance Portability and Accountability Act), SOX (Sarbanes-Oxley), GLBA (Graham Leach Bliley Act), CA SB 1386, FRCP (Federal Rules for Civil Procedure)

**Canada:** PIPEDA, Rule 30.02 Ontario Rules, Bill 198 Multilateral Instrument

#### Europe

Euro-SOX, MiFID (Markets in Financial Instruments Directive), European Union Data Protection Directive 95/46, European Union Directive 2006/24/EC

**UK:** Data Protection Act 1998, CPR (Civil Procedure Rules)

**Germany:** German Federal Data Protection Act, German Telecomms Data Retention Act, Criminal Procedures Act

**Switzerland:** Swiss Federal Data Protection (DPA), Basel II, stricter audit procedures, (SCO) Swiss Code of Obligations

#### Asia-Pacific

**Japan:** J-SOX, JPIPA (Japanese Personal Information Protection Act)

**India:** Right to Information Act, Companies Act, stricter audit procedures

**Singapore:** Companies Act

**Australia:** Privacy Act, APRA (Australian Prudential Regulation Authority) Guidelines, CLERP 9

#### Latin America

**Brazil:** Azaredo Law, Bill #6891/02

**Mexico:** Federal Freedom of Information Act, Ley Federal de Transparencia y Acceso a la Informacion Publica Gubernamental, Ley del Mercado de Valores

\*Frameworks tend not to be mandatory but are used to develop best practices which can map to specific regulations.

#### TREND MICRO™

Trend Micro Incorporated is a pioneer in secure content and threat management. Founded in 1988, Trend Micro provides individuals and organizations of all sizes with award-winning security software, hardware and services. With headquarters in Tokyo and operations in more than 30 countries, Trend Micro solutions are sold through corporate and value-added resellers and service providers worldwide. For additional information and evaluation copies of Trend Micro products and services, visit our Web site at [www.trendmicro.com](http://www.trendmicro.com).

#### TREND MICRO INC.

10101 N. De Anza Blvd.  
Cupertino, CA 95014

U.S. toll free: +1 800.228.5651

phone: +1 408.257.1500

fax: +1 408.257.2003

[www.trendmicro.com](http://www.trendmicro.com)

