



A Websense® White Paper

# Regulatory Compliance Highlights Value of Data Security Solutions for India

*The amendments to the Information Technology Act, 2000, of India have created additional and more stringent compliance requirements relating to cyber security, highlighting more than ever the value of data security solutions. Chief information officers and heads of technology charged with promoting compliance will need to pay even greater attention to their organizations' security needs as their organizations seek to ensure the confidentiality of information while providing necessary access to employees. Finding the right tools to meet compliance requirements, protect data, and provide safe access is increasingly becoming more critical.*

## Introduction

When confidential corporate information falls into the wrong hands, the consequences can be devastating. In today's hyper-competitive corporate world, road warriors have valid reasons to use an Internet connection at an airport or another unsecured point in a coffee shop. Changes introduced in the amendments to the Information Technology Act, 2000, have put the dual objectives of ensuring security as well as compliance firmly in the hands of the CIOs anywhere employees access data.

This white paper discusses some of the salient features of the Information Technology (Amendment) Act, 2008. The changes address concerns about data privacy and integrity, the prevention of security breaches, and the punishment of those found guilty of wrongdoing. The changes, especially in a new clause, 43A, added to Section 43 of the Act of 2000, have also shifted the focus toward data security rather than just the security of data repositories; and therefore, they have enhanced both the need for defining and securing sensitive data and the responsibility of technology heads for taking adequate measures to protect data against internal and external attacks.

## The Act: Then and Now

The Information Technology (IT) Act of 2000 provided the basic legal framework for electronic transactions; it fostered a degree of trust in the electronic medium of doing business.

It also established the legal sanctity of electronic documents and electronic signatures, making them acceptable to the government and as evidence in courts of law.

The act boosted e-governance and e-commerce through the establishment of certifying authorities that would issue digital signature certificates.

It created provisions for dealing with offenses such as computer hacking; facilitated the appointment of officers to fast-track civil court for decisions on compensation to victims of cyber attacks; and established a Cyber Appellate Tribunal to hear disputes under the act.

Corporations across industry sectors expected to see the act's amendments address concerns about data protection and create a more predictive legal environment that included electronic signatures, measures against data leakage, and cyber crimes.

Amendments to the IT Act have addressed some of the concerns raised by the industry about data protection: they create a legal environment in India that addresses breaches of confidentiality and integrity of data.

## Data Protection Clause

The original IT Act called for penalties for damaging computers and computer systems under section 43, widely interpreted as a regulation that upholds confidentiality of data and affords it protection. Unauthorized access to a computer, computer system, or computer network is punishable with a compensation of up to 10 million rupees. The amendment improves on these provisions by defining computer source code and including stealing of computer source code for which compensation can be claimed.

Data protection has now been made more explicit through clause 43A. This clause provides for compensation to an aggrieved person whose personal data, including sensitive personal data, may be compromised by a company during the time this data was under processing with the company and as a result of the company's negligent failure to protect such data due to a lack of implementing or maintaining reasonable security practices.

"Reasonable security practices and procedures" will constitute those practices and procedures that protect such information from unauthorized access, damage, use, modification, disclosure, or impairment as may be specified in an agreement between the parties or as may be specified by any law in force. In the absence of such an agreement or any law, the central government will prescribe security practices and procedures in consultation with professional bodies or associations.

Sensitive personal information may be prescribed by the central government in consultation with professional bodies or associations. In the context of outsourcing to India, this can be defined to be in line with compliance requirements of the EU Data Protection Directive and U.S. laws such as HIPAA or GLBA.

## Confidentiality and Privacy

On breach of confidentiality and privacy, the Act of 2000, restricted to those who gain access to an electronic record or document, has been enhanced with a new section that calls for punishment for disclosure of information in breach of a lawful contract.

Any person including an intermediary who has access to any material containing personal information about another person, as part of a lawful contract, and who discloses it without the consent of the subject person will be deemed in breach. Punishment will consist of imprisonment of up to three years, and/or a fine of 500,000 rupees. This may prove to be a strong deterrent to breaching data confidentiality.

These additions and changes aimed at improving data protection and making more stringent the punishment for breach of confidentiality might encourage greater business flow across international borders. Enterprises may become more confident about their global data traffic coming into or even passing through India.

## Cyber Crimes

Crime-specific subsections on hacking and obscene material have been updated in the existing sections of the original act, making cyber crimes punishable. A section has also been rewritten to include cyber terrorism. Further, the requirement of a deputy superintendent of police (DSP) to investigate cyber crimes has been relaxed, and an inspector is now deemed competent to investigate crimes under this act.

Traffic data, logs, and information will be required to be maintained by intermediaries for cyber security according to procedures and safeguards that will be prescribed by the central government. This will ensure the availability of cyber forensic data, which is essential for investigation and prosecution of cyber crimes.

Cyber forensic evidence is critical to trials of cyber criminals. With the changes to the act, the central government may specify any department, body, or agency as an examiner of electronic evidence for the purposes of submitting expert opinion on electronic form evidence before any court.

## New Definitions

New definitions in the amended version include those for communication devices, cyber cafés, cyber security, electronic signature, and the Indian Computer Emergency Response Team.

A communication device in the act could be a cell phone, personal digital assistant, a combination of both, or any other device used to communicate, send, or transmit any text, video, audio, or images.

Cyber cafés are defined as any facility from where access to the Internet is offered by anybody in the ordinary course of business to the members of the public.

Some definitions of terms, including computer network, information, and intermediary, have been redefined to enhance clarity. For example, an intermediary with respect to an electronic record is now any person who on behalf of another person receives, stores, or transmits that record or provides any service with respect to that record. Therefore, the definition also covers service providers in areas such as telecommunications and online markets.

The changes also delineate the conditions under which intermediaries will not be liable; and an intermediary, when asked by a designated government agency, has to provide the required technical assistance to enable online access or to secure and provide online access to the computers generating, transmitting, receiving, or storing traffic data or information. Failure to do so shall make an intermediary liable to punishment by imprisonment of up to three years and a fine.

Intermediaries will also have to provide the assistance that the Indian Computer Emergency Response Team needs in doing its job. The nodal agency prescribes the procedures for this.

## Nodal Agency

Changes made to the provisions of the IT Act of 2000 now include any computer that is part of a critical information infrastructure, and a national nodal agency has been designated for the protection of critical information infrastructure. This agency will be responsible for all measures including the research and development needed for protecting vital information networks, computer systems, and other elements of the infrastructure.

The Indian Computer Emergency Response Team will perform all functions relating to cyber security, including responding to cyber security incidents. Service providers, intermediaries, companies, and others will have to provide information to the agency when required and in accordance with procedures that shall be prescribed by this nodal agency.

## The Right Tools

The full impact of the explosion of applications, not just Web-based but also those available within organizations across industry sectors, on enterprises and their information security is yet to be understood. As chief information officers grapple with the need for reasonable policy controls — ensuring the safety of their networks while providing adequate access to applications for productive work to happen — choosing an effective data security tool becomes crucial. The right one can enable business workflow by reliably securing data and ensuring compliance no matter how or where the data is accessed.

Reliable data security tools that also aid compliance will be welcomed by IT administrators tasked with sifting through a myriad set of new dynamic applications used by employees. That the new clause on data security squarely places the onus of securing sensitive data on the organization will also make chief information officers and chief information security officers ever more vigilant.

When choosing data security solutions, organizations will look for tools that are able to dynamically classify content, identifying good and keeping out the bad, in real time. Finding the right solution will be of paramount importance.

## Websense® Solutions

Websense data loss prevention (DLP) solutions help secure confidential data and manage risk and compliance. Websense DLP technologies benefit from the unified content security and analysis offered by the Websense TRITON™ solution and provide market-leading DLP capabilities designed to secure sensitive information and intellectual property, as well as manage and enforce regulatory requirements. Supporting a wide range of deployment options, Websense DLP solutions enable organizations to deploy the DLP solution that best meets their needs with reduced cost and complexity.

### Help Prevent Loss of Sensitive Data

With the ability to identify and monitor organizations' sensitive data, Websense DLP solutions help prevent data loss through data transmission and exchange including email, Web, USB, and other channels.

### Increase Visibility Into Where Data is Sent and Stored

Websense DLP solutions provide visibility into where data resides, where it's sent, and by whom.

### Meet Regulatory Compliance

Simplify the task of helping ensure regulatory compliance with built-in templates for financial, health care, and other regulated industries by using Websense DLP solutions.

### Flexible Product Options

Websense Data Security Modules - Providing flexibility to meet the specific requirements of each organization, Websense data loss prevention solutions comprise four unique modules. The modular design enables staged rollouts that best meet organizations' specific needs.

- **Websense Data Monitor** - Provides visibility into network traffic and compliance and risk reporting.
- **Websense Data Protect** - Includes Websense Data Monitor and adds on enforcement capabilities to protect regulated information.
- **Websense Data Discover** - Scans file storage systems to identify areas of risk, where data loss might occur.
- **Websense Data Endpoint** - Extends coverage to the client for offline protection.

Websense Data Security Suite - Designed for enterprise DLP deployments, Websense Data Security Suite includes the four integrated modules, managed under a single policy framework.

For more information on Websense data loss prevention solutions, visit [www.websense.com](http://www.websense.com).

## CIO Speak: The Significance of 43A

The Amendments shift the focus away from traditional approaches to “data” security, says Murli Nambiar, Group Chief Information Security Officer at Reliance Capital. They have also become more specific in apportioning responsibility for that security, he says, in this interview.

### Q. In what way did the amendments help increase data security, in your view?

**Nambiar:** Previously Section 43 was not very specific towards the obligations of a company to protect and secure data in their possession. Clause 43A is very specific toward the obligation of companies to secure the data in their possession. According to the amendment, if the data is misused due to a company being negligent in implementing and maintaining reasonable security practices and procedures, the affected person or corporate can claim damages.

### Q. How are you at Reliance Capital using data security solutions to comply with the act/amendments or even taking advantage of the changes in the act to strengthen your data security?

**Nambiar:** Reliance Capital adopted a four-pronged strategy to address this and comply with the act – we initiated a “data flow analysis” where all sensitive data was traced across the environment. Once the data was identified, we classified them according to our data classification policy.

After changes to the act were made, we secured the documents with “Rights Management” software, which helped to assign low level access rights like defining who can view, print, edit, and even expire documents after a specific period of time.

The confidential data were then fingerprinted on our DLP solution, which helped to block data being sent out through various channels like emails, Web, USB, etc., even when the endpoint was not connected to our network.

All mobile devices were secured with encryption software at disk level and data on removable media was encrypted when they were copied onto it.

### Q. Any other comments you’d like to add in this context (for instance on why the amendments are important)?

**Nambiar:** The amendment is quite important, because it takes the focus away from traditional approaches of security and puts focus on “data” security, i.e., focus on data rather than containers it’s stored in. It’s also important for the initial data flow analysis phase to be done thoroughly and completely to identify the core data which needs to be secured rather than concentrating efforts on all data within the environment.

Compiled by IDG Media Custom Solutions Group

Sources include the Information Technology (Amendment) Act, 2008; and Data Protection and Cyber Crimes Under the Information Technology Amendment Bill, 2008, Data Security Council of India.