

RSA[®]Conference2015

San Francisco | April 20-24 | Moscone Center

SESSION ID: LAW-R04

Following the Sun: A Worldwide View of Cybersecurity Laws and Regulations

CHANGE

Challenge today's security thinking



MODERATOR:

Jessica Gulick

Chief Strategist
CSG Invotas
@CyberRiskLady

PANELISTS:

Gene Fredriksen

Chief Information Security Officer
PSCU
@PSCUForward

James Halpert

Partner, Co-Chair Cybersecurity Practice
DLA Piper
@DLA_Piper

Larry Clinton

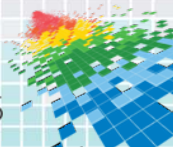
President and Chief Executive Officer
Internet Security Alliance
@ISAlliance

Overall Key Challenges & Highlights

- ◆ You can't develop a ground up set of controls for each country, so how to define the 80 – 20 requirements that will drive your base standards?
- ◆ There are finite company legal and compliance resources. How do you make the best use of those resources?
 - ◆ Internal resources
 - ◆ Outside counsel
 - ◆ Information service
- ◆ Regulations are dynamic. How do you keep your advice current? Follow changes? How do you identify countries most apt to change?

Use Case Examples

- ◆ Global DLP:
 - ◆ You are the Project Manager for an initiative to implement a global DLP strategy. The strategy includes the monitoring of email for keywords related to company intellectual property.
- ◆ M&A Activity in Russia
 - ◆ You are the security and compliance lead for an acquisition based expansion into Russia. Since the company will be a manufacturing partner, Trade Secret information will be involved.
- ◆ Breach Response
 - ◆ Your company has suffered a breach that has touched employees and customers in multiple countries. You are the lead for investigating the hacking incident which may involve the theft of personal information and company intellectual property.



Use Case: DLP (restrictions on monitoring)

Germany, India, Korea ▾

1. Cybersecurity Mandates

2. Security Standards

3. Restrictions on Security Technologies


4. Restrictions on Monitoring of Security Issues

A. Overview


B. Practical Enforcement Risk

C. Degree of Activity that Triggers Enforcement


5. Security Breach Notice Requirements


Germany
Last modified January 26, 2015

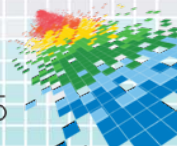
There are no special provisions concerning monitoring and detection, but general statutory provisions apply. In particular, monitoring and detection measures must not violate the [German Federal Data Protection Act \(Bundesdatenschutzgesetz, BDSG\)](#). Monitoring of personal data without consent of the data subject is only possible under exceptional conditions (eg. if there is reasonable suspicion that criminal actions are imminent or to safeguard legitimate interests of the company and there is no reason to assume that the data subject has an overriding legitimate interest in ruling out the possibility of processing). Also, the monitoring must not violate the [German Telecommunication Act \(Telekommunikationsgesetz, TKG\)](#) and in particular not violate the telecommunication secrecy. Monitoring may also be subject to the consent of the works council, according to sec. 87 of the Industrial Relations Law ([Betriebsverfassungsgesetz](#)).


India
Last modified January 26, 2015




Private use of security technologies to intercept or monitor any communication is prohibited. There is no specific definition of security technologies. However, in the context of cybersecurity, it may include illegal acts of interception, monitoring, decryption or blocking. Such private use of security technologies is prohibited in public. Use of such technologies in the workplace may be seen as a violation of the right to privacy. There is no legal provision covering the monitoring of employee communications for security issues (eg. to detect malware or data exfiltrations); therefore, if employers provide notice to employees about such monitoring, they are unlikely to be viewed as violating the right to privacy.



Korea
Last modified January 26, 2015


Limited restrictions, mostly related to intercepting communications without all necessary consents or a warrant, or violation of communications privacy without consent.




Use Case: M&A Activity in Russia


[HOME](#) [MARKET INSIGHT](#) [CONTRIBUTORS](#) [ABOUT](#) [CONTACT US](#) 

Jim 

Russia 


- 1. Cybersecurity Mandates
- 2. Security Standards
- 3. Restrictions on Security Technologies**
 - A. Overview**
 - B. Practical Enforcement Risk
 - C. Degree of Activity that Triggers Enforcement
- 4. Restrictions on Monitoring of Security Issues
- 5. Security Breach Notice Requirements

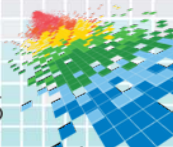
3.A. Overview

 **Russia** Last modified January 26, 2015

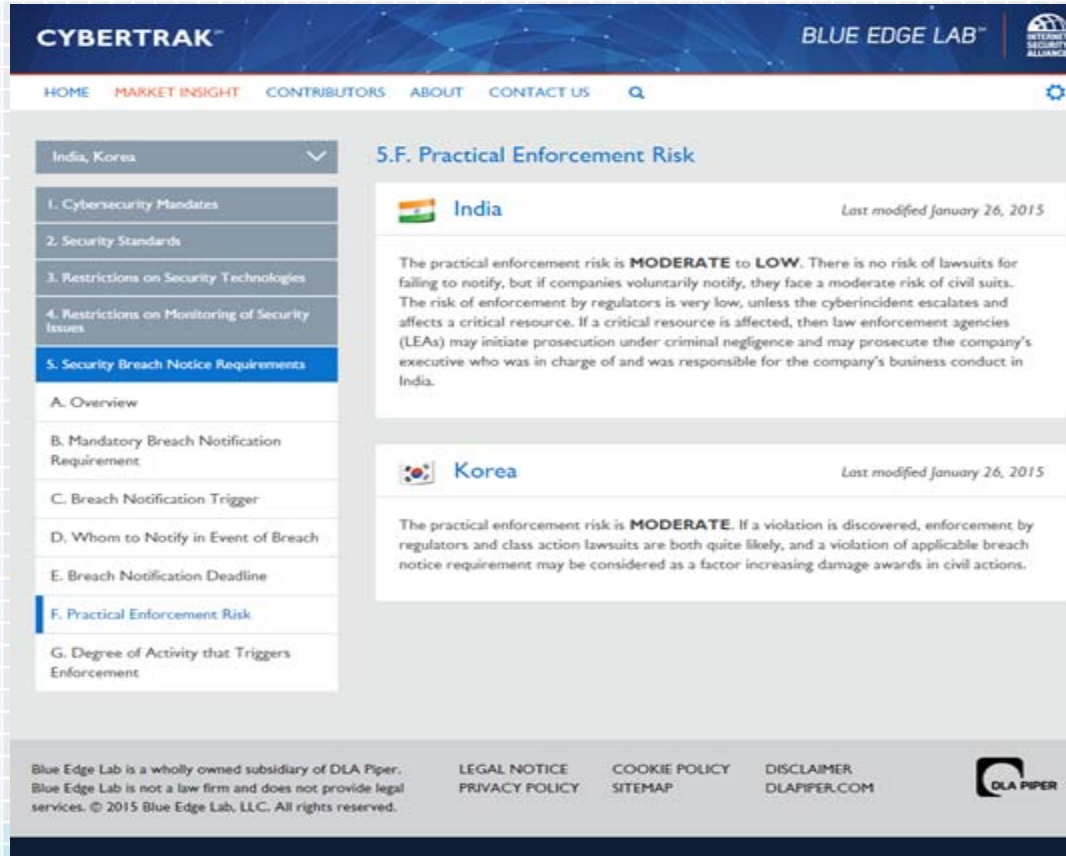
Licensing requirements. Export and use of encryption technologies in Russia require a state license issued by the Federal Security Service upon submission by the applicant of information on the technical parameters of the encryption technologies. Additionally, telecom networks are subject to state regulatory requirements concerning compliance with certain technical parameters, such having the ability to interact with other networks and being accessible to state security authorities in case of need (legal interception rule).

<https://www.blueedgelab.com/subscriptions/cybertrak/countries/?t=restrictions-on-security-technologies&c=RU>





Use Case: Breach Enforcement



CYBERTRAK™ BLUE EDGE LAB™ INTERNET SECURITY ALLIANCE

HOME MARKET INSIGHT CONTRIBUTORS ABOUT CONTACT US

India, Korea

- 1. Cybersecurity Mandates
- 2. Security Standards
- 3. Restrictions on Security Technologies
- 4. Restrictions on Monitoring of Security Issues
- 5. Security Breach Notice Requirements**
 - A. Overview
 - B. Mandatory Breach Notification Requirement
 - C. Breach Notification Trigger
 - D. Whom to Notify in Event of Breach
 - E. Breach Notification Deadline
 - F. Practical Enforcement Risk**
 - G. Degree of Activity that Triggers Enforcement

5.F. Practical Enforcement Risk

India

Last modified January 26, 2015

The practical enforcement risk is **MODERATE to LOW**. There is no risk of lawsuits for failing to notify, but if companies voluntarily notify, they face a moderate risk of civil suits. The risk of enforcement by regulators is very low, unless the cyberincident escalates and affects a critical resource. If a critical resource is affected, then law enforcement agencies (LEAs) may initiate prosecution under criminal negligence and may prosecute the company's executive who was in charge of and was responsible for the company's business conduct in India.

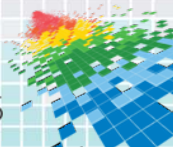

Korea

Last modified January 26, 2015

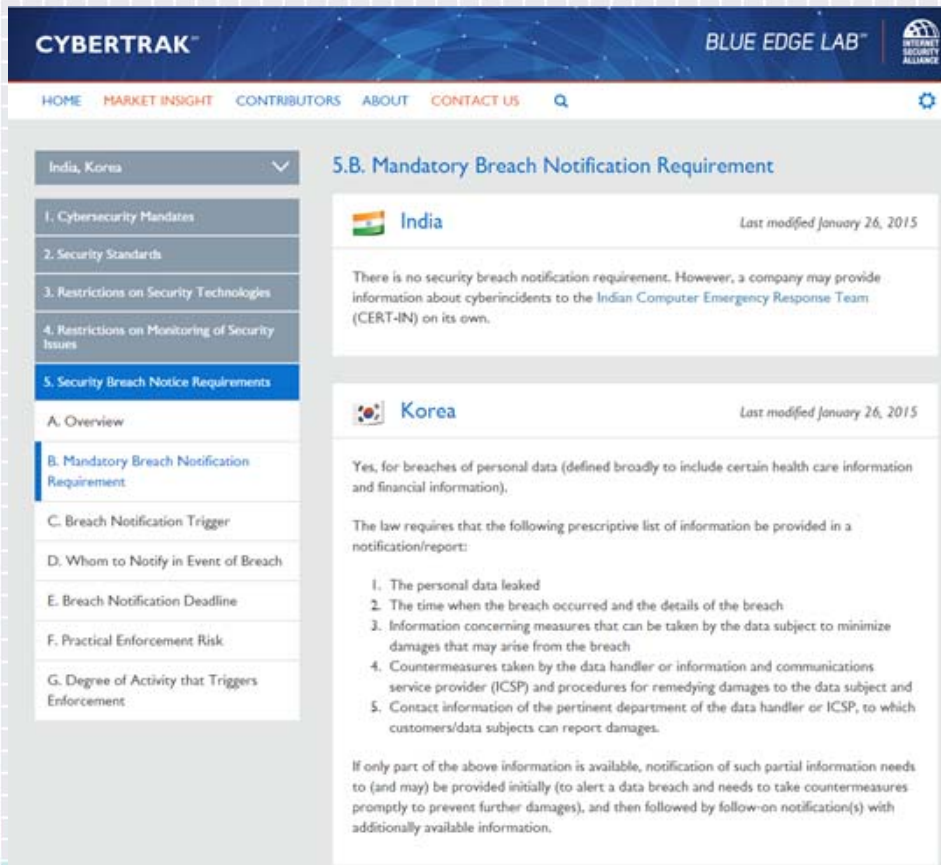
The practical enforcement risk is **MODERATE**. If a violation is discovered, enforcement by regulators and class action lawsuits are both quite likely, and a violation of applicable breach notice requirement may be considered as a factor increasing damage awards in civil actions.

Blue Edge Lab is a wholly owned subsidiary of DLA Piper. Blue Edge Lab is not a law firm and does not provide legal services. © 2015 Blue Edge Lab, LLC. All rights reserved.

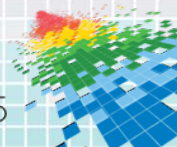
LEGAL NOTICE PRIVACY POLICY COOKIE POLICY SITEMAP DISCLAIMER DLAPIPER.COM




Use Case: Breach Enforcement



The screenshot shows the CYBERTRAK website interface. At the top, there is a navigation bar with links for HOME, MARKET INSIGHT, CONTRIBUTORS, ABOUT, and CONTACT US, along with a search icon and a gear icon. The main content area is titled '5.B. Mandatory Breach Notification Requirement'. On the left, there is a sidebar menu with a dropdown for 'India, Korea' and a list of categories including 'Cybersecurity Mandates', 'Security Standards', 'Restrictions on Security Technologies', 'Restrictions on Monitoring of Security Issues', and 'Security Breach Notice Requirements'. The 'Security Breach Notice Requirements' category is expanded to show sub-sections: 'A. Overview', 'B. Mandatory Breach Notification Requirement', 'C. Breach Notification Trigger', 'D. Whom to Notify in Event of Breach', 'E. Breach Notification Deadline', 'F. Practical Enforcement Risk', and 'G. Degree of Activity that Triggers Enforcement'. The main content area displays two sections: 'India' and 'Korea'. The 'India' section states that there is no security breach notification requirement, but companies may provide information to the Indian Computer Emergency Response Team (CERT-IN). The 'Korea' section states that breaches of personal data require notification and lists five prescriptive items: 1. The personal data leaked, 2. The time when the breach occurred and the details of the breach, 3. Information concerning measures that can be taken by the data subject to minimize damages, 4. Countermeasures taken by the data handler or information and communications service provider (ICSP) and procedures for remedying damages, and 5. Contact information of the pertinent department of the data handler or ICSP.



Use Case: Breach Enforcement

CYBERTRAK™
BLUE EDGE LAB™



HOME MARKET INSIGHT CONTRIBUTORS ABOUT CONTACT US Q

India, Korea


1. Cybersecurity Mandates
2. Security Standards
3. Restrictions on Security Technologies
4. Restrictions on Monitoring of Security Issues
5. Security Breach Notice Requirements

- A. Overview
- B. Mandatory Breach Notification Requirement
- C. Breach Notification Trigger
- D. Whom to Notify in Event of Breach
- E. Breach Notification Deadline
- F. Practical Enforcement Risk
- G. Degree of Activity that Triggers Enforcement

5.C. Breach Notification Trigger


India
Last modified January 26, 2015

The trigger is a cybersecurity incident, which has been defined as “any real or suspected adverse event in relation to cybersecurity that violates an explicitly or implicitly applicable security policy resulting in unauthorised access, denial of service or disruption, unauthorised use of a computer resource for processing or storage of information or changes to data, information without authorisation.” Rule 2(h) of Indian Computer Emergency Response Team (CERT-IN) Rules.


Korea
Last modified January 26, 2015

Breach of any personal data protected by the Personal Information Protection Act (PIPA) or the Act on Promotion of IC Network Utilization and Information Protection (IC Network Act) (no encryption exception, or employee exception is available)

A “data breach” is defined as (i) the loss of control over personal data which is not due to the application of a pertinent law or discretion by the data handler or (ii) unauthorized access to personal information processing systems such as databases containing personal data.


The laws do not prescribe, and thus it is not necessarily construed that personal data protected by the PIPA or IC Network Act are limited to personal data of Koreans only, aside from practical enforceability issues.

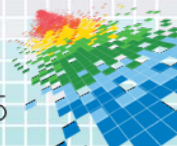
Blue Edge Lab is a wholly owned subsidiary of DLA Piper. Blue Edge Lab is not a law firm and does not provide legal services. © 2015 Blue Edge Lab, LLC. All rights reserved.

LEGAL NOTICE
PRIVACY POLICY


COOKIE POLICY
SITEMAP

DISCLAIMER
DLAPIPER.COM





Use Case: Breach Enforcement

CYBERTRAK™
BLUE EDGE LAB™


HOME MARKET INSIGHT CONTRIBUTORS ABOUT CONTACT US Q

India, Korea

1. Cybersecurity Mandates

2. Security Standards

3. Restrictions on Security Technologies

4. Restrictions on Monitoring of Security Issues

5. Security Breach Notice Requirements

A. Overview

B. Mandatory Breach Notification Requirement

C. Breach Notification Trigger


D. Whom to Notify in Event of Breach

E. Breach Notification Deadline


F. Practical Enforcement Risk

G. Degree of Activity that Triggers Enforcement

5.D. Whom to Notify in Event of Breach


India
Last modified January 26, 2015

Indian Computer Emergency Response Team (CERT-IN)


Korea
Last modified January 26, 2015


PIPA: Under the Personal Information Protection Act (PIPA):

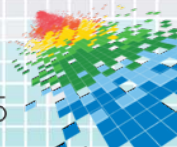
1. Data subjects and
2. Ministry of Security and Public Administration (MOSPA) (or the National Information Security Agency (NIA) or Korea Information Security Agency (KISA) as delegated by the MOSPA), if 10,000 or more data subjects are affected.

IC Network Act: Under the Act on Promotion of IC Network Utilization and Information Protection (IC Network Act), information and communications service providers (ICSPs) must notify:

1. Users of information and communication services and
2. The Korea Communications Commission (KCC) (or KISA as delegated by the KCC).

Under the IC Network Act, there is no threshold for notification, so all breaches must be reported to the regulator.

Blue Edge Lab is a wholly owned subsidiary of DLA Piper. Blue Edge Lab is not a law firm and does not provide legal
LEGAL NOTICE
PRIVACY POLICY
COOKIE POLICY
SITEMAP
DISCLAIMER
DLAPIPER.COM




Apply: Operationalizing Compliance

- ◆ Top Take-Aways
 - ◆ Be prepared: Access to global legislation information across multiple countries
 - ◆ Stay aware: Get notified of significant changes
 - ◆ Understand: Know where you are most at risk for liability
 - ◆ Engage: Influence the legislation
 - ◆ Apply: Shape your data strategy to maximize return and minimize legal risks and penalties
 - ◆ Operationalize: In-house staff, outside council, automated solutions, and hybrid

