How to Legally Deal with a Security Breach at Work

sflc.in

Biju K Nair
Advocate & Executive Director, SFLC.in

Legal framework in India around security breaches

- Information Technology Act, 2000
- Section 43 - Penalty for damage to Computer System
  - accesses or secures access to such computer, computer system or computer network;
  - downloads, copies or extracts any data, computer data base;
  - introduces or causes to be introduced any computer contaminant or computer virus;
  - disrupts or causes disruption of any computer;
  - denies or causes the denial of access to any person authorised to access

(Contd.)

- provides any assistance to any person to facilitate access to a computer, computer system or computer network in contravention of the provisions of this Act;

- charges the services availed of by a person to the account of another person by tampering with or manipulating any computer.

- PENALTY: Liable to pay damages by way of compensation an amount not more than one crore to affected person.

Protected systems

- Computer resource which directly or indirectly affects the facility of Critical Information Infrastructure to be a protected system.

- "Critical Information Infrastructure" means the computer resource, the incapacitation or destruction of which , shall have debilitating impact on national security, economy, public health or safety.

- Breach of Protected System - Imprisonment of either description for a term which may extend to ten years and shall also be liable to fine

Incident response – national agency

- Indian Computer Emergency Response Team – CERT-In (Section 70B, IT Act)
- Mandate of CERT-In:
  - Collection, analysis and dissemination of information on cyber incidents
  - Forecast and alerts of cyber security incidents
  - Emergency measures for handling cyber security incidents
  - Coordination of cyber incidents response activities
  - Issue guidelines, advisories, vulnerability notes and white papers relating to information security practices, procedures, prevention, response and reporting of cyber incidents
  - Such other functions relating to cyber security as may be prescribed

Cyber security incident and breach

- Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013
- “Cyber security incident” means any real or suspected adverse event in relation to cyber security that violates an explicit or implied security policy resulting in unauthorized access, denial of service/ disruption,unauthorized use of a computer resource for processing or storage of information or changes to data, information without authorization
- Cyber security breaches” means unauthorized acquisition by a person of data or information thatcompromises the confidentiality, integrity oravailability of information maintained in a computer resource

Mandatory reporting of cyber security incidents

- Who must report?
  - Body corporates
  - Data centers
  - Intermediaries
  - Service providers
- Incidents have to be reported within a reasonable time of occurance or noticing the incident to have scope for timely action.

(Contd.)

- What must be reported?
  - Attacks on servers such as Database, Mail and DNS and network devices such as Routers
  - Attacks on critical infrastructure, SCADA systems and wireless network.
  - Attacks on applications such as e-Governance, e-Commerce, etc.
  - Compromise of critical systems / infrastructure
  - Defacement of websites or intrusion into a website and unauthorized changes such as inserting malicious code, links to external websites, etc.

(Contd.)

- Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks
- Identity theft, spoofing and phishing attacks
- Malicious code attacks such as spreading of virus/worm/trojan/botnets/spyware
- Targeted scanning/probing of critical networks/systems
- Unauthorized access of IT systems/data

- Reporting any other type of cyber security incident is optional - can be done by individuals, organizations, corporate entity.

Procedure for reporting a breach to CERT-In

- Provide as much information as possible, including:
  - Time of occurance of the incident
  - Information regarding affected system/network
  - Symptoms observed
  - Relevant technical information such as security systems deployed, actions taken to mitigate the damage, etc.
- Incident reporting form: http://cert-in.org.in/PDF/certinirform.pdf

(Contd.)

- Email the information to: incident@cert-in.org.in
- Phone call to: +91-1800-11-4949
- Fax to: +91-1800-11-6969
- Post to: CERT-In, Electronics Niketan, CGO Complex, New Delhi – 110003

Support from CERT-In

- Rule 11 of 2013 Rules.
- Ultimate responsibility of the security of the computer resource rests with the owner of the computer resource.
- It is not certain that CERT-In will provide support in case of cyber security incidents.
- Support is provided on the basis of availability of resources and an order of priotity based on the threat posed by different kinds of security incidents.

Order of priority for providing support – CERT-In

1) Threats to the physical safety of human beings due to cyber security incidents;

2) Cyber incidents and cyber security incidents of severe nature (such as denial of service, distributed denial of service, intrusion, spread of computer contaminant) on any part of the public information infrastructure including backbone network infrastructure;

3) Large scale or most frequent incidents such as identity theft, intrusion into computer resource, defacement of websites, etc.;

4) Compromise of individual user accounts on multi-user systems;

5) Types of incidents other than those mentioned above will be prioritised according to their apparent severity and extent.

Point of contact - mandatory

- Who should appoint a point of contact [R. 17 of 2013 rules]:
  - Service providers
  - Intermediaries
  - Data centers
  - Body corporate
- Information relating to the point of contact must be sent to CERT-In and kept updated regularly.
- If CERT-In wants to ask you for some information, they will contact your designated point of contact.

Disclosure of information by CERT

- CERT-In is not allowed to disclose any information which may lead to identification of those affected by cyber security incidents without their explicit written consent or orders of Indian competent courts or where it is necessary for defence of India, security of the State, public order, preventing incitement to commit an offence, enhancing cyber security in the country, etc.

Compensation for failure to protect data [S. 43A – IT Act]

- If wrongful gain or loss is caused to anyone as a result of sensitive **personal data or information** being breached or leaked from a body corporate because of neligence in implementing and maintaining resonable security practices and procedures.

- PENALTY - Liable to pay compensation of up to Rs. 5 crore to the affected person.

Penalty for failure to furnish information, return, etc.

- If you are required by CERT-In to furnish any information, books or other documents within a specific time and you don‘t do it, you will be liable to a penalty of up to Rs. 5000 per day. [S. 45(b), IT Act]

- If you do not maintain books of account or records, you will liable to a penalty of up to Rs. 10,000 for every day during which the failure continues. [S. 45(c), IT Act]

- For other contraventions, you may be liable to pay a compensation or a penalty of up to Rs. 25,000 to the person affected. [S. 45, IT Act]

Insurance

- IRDAI has made an exposure draft titled “Information and Cyber Security Framework for Insurance Sector“ in 2017.

- These guidelines are applicable to all insurers.

- In case of intermediaries and other regulated entries with whom the policyholder information is being shared, it would be the responsibility of insurers to ensure that adequate mechanisms are put in place to ensure that the issues related to information and cyber security are addressed.

(Contd.)

- Timelines for implementation
  - 30th Apr 2017 - Appointment/ designation a suitably qualified and experienced Senior Level Officer exclusively as Chief Information Security Officer (CISO) who will be responsible for articulating and enforcing the policies to protect their information assets and formation of Information Security Committee (ISC)
  - 30th Jun 2017 - Preparation of Gap Analysis report
  - 30th Jun 2017 - Formulation of Cyber Crisis Management Plan

Banking

- RBI in 2011- Guidelineson Information Security, Electronic Banking, TechnologyRisk Management and Cyber Frauds (G.Gopalakrishna Committee) 11 April 2011; measures suggested for implementation cannot be static and banks need to pro-actively create/fine-tune/modify their policies, procedures
- RBI in 2016, issued a Circular on Cyber Security Framework in Banks
- Cyber Security incidents must be reported to RBI within 2-6 hours.
- Center for AnalysisofRisks and Threats (IB -CART) setu by IDRBT.
- Self Assesement of Gaps to be done by Banks and to be submitted to RBI by July 31, 2016
- Annexure 3 of the circular contains the template and form for reporting such incidents.
- Despite mechanism, 3.2 million cards compromised - http://economictimes.indiatimes.com/industry/banking/finance/banking/3-2-million-debit-cards-compromised-sbi-hdfc-bank-icici-yes-bank-and-axis-worst-hit/articleshow/54945561.cms

Securities and exchange

- Cyber Security and Cyber Resilience framework of Stock Exchanges, Clearing Corporation and Depositories, 2015 – CIR/MRD/DP/13/2015

- Applicable to Market Infrastructure Institutions (MIIs) in the securities market.

- Quarterly reports containing information on cyber attacks and threats experienced by MII and measures taken to mitigate vulnerabilities, threats and attacks including information on bugs / vulnerabilities / threats that may be useful for other MIIs, should be submitted to SEBI.

- Cyber Security and Cyber Resilience framework of National Commodity Derivatives Exchanges, 2016 – SEBI/HO/CDMRD/DEICE/CIR/P/2016/0000000044

    - Extends the application of ‘Cyber Security and Cyber Resilience framework of Stock Exchanges, Clearing Corporation and Depositories‘ to MIIs in the commodity derivatives market.

Cases

- OYO v/s Zostel - Delhi High Court 2015
  - OYO filed a case against Zostel claiming that Zostel had copied data from OYO.The data was allegedly taken by insiders as OYO‘s employees had, as per the claim, taken proprietary software from OYO before leaving to join Zostel.
  - Delhi High Court issued a stay order against Zostel in this case.
  - OYO and Zostel settled; Oyo bought Zostel

How to produce electronic evidence in Court

- Section 65B of Indian Evidence Act, 1872 explains how elecronic evidence to be produced.

- Landmark Judgement of Supreme Court: Anvar v. P. K. Basheer.

Procedure for production of electronic evidence

- Section 65B(4) of the Evidence Act. In any proceedings pertaining to an electronic record, following conditions to be satisfied:
  - A certificate which identifies the electronic record containing the statement;
  - Certificate must describe the manner in which the electronic record was produced;
  - Certificate must furnish the particulars of the device nvolved in the production of that record;
  - Certificate must deal with the applicable conditions mentioned under Section 65B(2) of the Evidence Act;
  - Certificate must be signed by a person occupying a responsible official position in relation to the operation of the relevant device.

Thank you!